STATEWIDE INFORMATION TECHNOLOGY ARCHITECTURE

Architecture: Strategic Network Architecture

Effective Date: December 1, 2006

Approved: Richard B. Clark

I. Architecture Purpose

The Strategic Network Architecture developed by the Department of Administration Information Technology Services Division (ITSD) describes the network framework that will be used by SummitNet, the state's enterprise telecommunications network, to support design requirements, deployment of new network services and evolving technology. The architecture provides the vision and direction for a predictable, scalable, reliable and secure network environment.

The architecture will support the administrative and business functions of all state agencies, including the University System.

II. Definitions

Architecture: An architecture is a blueprint that defines the business, the information necessary to operate the business, the technologies necessary to support the business operations, and the transitional processes necessary for implementing new technologies in response to the changing business needs.

III. Closing:

For questions on the Strategic Network Architecture, e-mail ITpolicy@mt.gov, or, contact the Information Technology Services Division at:

Chief Information Officer
PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

The technical contact at the Information Technology Services Division for this architecture is:

Steve Noland, Network Research and Design
PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

IV. Administrative Use

History Log	
Approved Date:	December 1, 2006
Effective Date:	December 1, 2006
Change and Review Contact:	ITpolicy@mt.gov
Review:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	July 1, 2009
Last Review/Revision:	
Changes:	

Department of Administration
Information Technology Services Division

STRATEGIC NETWORK ARCHITECTURE

Document Owner: **State of Montana**

Previous Documents: **NONE**
Related Documents: **None**

Distribution: **State of Montana**

ISSUE & AMENDMENT RECORD

Version	Date	Revised By	Comments
Draft 0.1	8/14/2006	J.Lester	New Document created by Technical Design Authority

State of Montana furnishes this technical design specification.

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

TABLE OF CONTENTS (CONTINUED)

TABLE OF CONTENTS (CONTINUED)

1.0 INTRODUCTION

Modern enterprise telecommunication networks must be scalable and flexible in an increasingly dynamic and complex service environment. They must reliably, securely and simultaneously transport many different types of information such as voice, video and data. These networks must extend across distances easily to support all types of user communities from large State agencies to small remote agency offices with one or two users. The network must be engineered with the timing, synchronization, and intelligence necessary to support the State of Montana's entire communication system.

Customers of today's increasingly complex networks require systems that provide consistent performance and operational features, and at the same time enable rapid deployment of new services and applications throughout the entire network.

To satisfy these requirements, networks today must offer transport services that are:

- Redundant
- Reliable
- Predictable
- Secure

The ability to offer converged technologies is one of the main benefits of a reliable, predictable and redundant network. In a network where technologies converge, information such as electronic data, voice conversations and live video all traverse the same transport medium in a model similar to commuters on a subway system. Today the State of Montana, Department of Administration, Information Technology Services Division (ITSD) maintains three separate subways to transport data, voice, and video. When the video transport is not in use, it simply sits idle, and is not utilized for data or voice. In a converged network design if at any time the video technology is not in use, data and voice have additional bandwidth available.

Three major sections of this document describe the network architectures necessary to support converged technologies. They are:

- Network Transport
- Network Services
- Network Support

The Network Transport section addresses network transport architecture supported today, and the upgrades necessary to design, implement, support, manage, and secure a comprehensive enterprise network for the State of Montana.

The Network Transport section also addresses the upgrades necessary to provide transport services based on Montana's six connection models:

- State Agencies
- University System
- Local Government (City/ County)
- K-12 Schools and School Districts
- Vendors/ Contractors
- Remote Access

The Network Services section addresses the services that must be in place and functioning properly in order for the State of Montana to provide comprehensive information services to its consumers. The areas discussed in the Network Services section are:

- IP Protocol Routing
- Multicast Routing
- Domain Name Services (DNS) and Dynamic Host Configuration Protocol (DHCP)
- Wireless Technologies
- Unified Messaging

Network management and operations are addressed in the Network Support section to be supplied in a subsequent revision.

The three major sections combined together provide the reader a good understanding of the strategic network architecture direction for the State of Montana.

2.0 NETWORK TRANSPORT

Today the State of Montana operates a single telecommunications network across Montana for State agencies and universities referred to as SummitNet (State and Universities of Montana Multiprotocol Network).

This section addresses the network transport architecture of SummitNet and what is necessary to meet the State and Universities growing telecommunications transport needs of the future.

2.0.1 GOALS

The network transport layers primary goal is to provide a physical infrastructure that is scalable, stable, and secure.

The first goal is easily achievable with the 3-layer hierarchy of the network transport layer. The three layers and their objectives are:

High-Speed Core Network Layer:

1. Transport the IP packets as quickly as possible, as far as possible, with minimum delay

Distribution Network Layer:

1. Move packets to/from the outside edge of the core routers, and to/from the agencies
2. Facilitate the scaling of the State of Montana Intranet

Access Network Layer:

1. Provide all State of Montana users access to the resources and services found throughout the State of Montana Intranet
2. Connect the agency Intranets

When the objectives are combined together it is possible to achieve the final goal of converged technologies.

The second goal of the network transport is to provide a secure network for the State of Montana. This is accomplished by inspecting all non-trusted data before it is placed onto the trusted network.

2.0.2 ISSUES AND CONCERNS

Use of the present State of Montana network assets is a major consideration in designing the new State of Montana converged network to meet the strategic network plan objectives and deliverables. To meet these design principles, the State of Montana must upgrade or replace a significant portion of the existing interconnection components and media.

2.0.3 PRINCIPLES

There are four basic principles of the Network Transport design model discussed in this section. These principles combined together achieve the goals as outlined in the Network Transport section 2.0.1. The principles are:

- Hierarchy
- Stability
- Scalability
- Security

HIERARCHY PRINCIPLE:

The top layer of the hierarchy, the State of Montana core, is the enterprise high-speed network. Its primary objective is to provide high-speed transport of the State of Montana's Intranet data. To accomplish this, the enterprise high-speed network layer transports the IP packets as quickly as possible, as far as possible, with a minimum of delay. This layer has no implementation of policy, and has minimal straightforward security.

The middle layer or distribution layer is the interconnection point into the State of Montana's core. Its primary objective is to move packets to/from the outside edge of the core routers, to/from the agency interconnect, and allow for scaling of the State of Montana Intranet. Its second objective is to provide security for the State of Montana Intranet at interconnection points. This is achieved by implementing policies.

The bottom layer or access layer provides an interconnection point into the State of Montana Intranet for the user. Its primary objective is to provide secured user connectivity into the State of Montana Intranet. The second objective is to divide the traffic up into categories or queues. Each queue has a predefined priority and bandwidth allocation within the network. Traffic such as voice or video get a higher priority queue in the network than does a file transfer.

HIERARCHY PRINCIPLE NETWORK MODEL

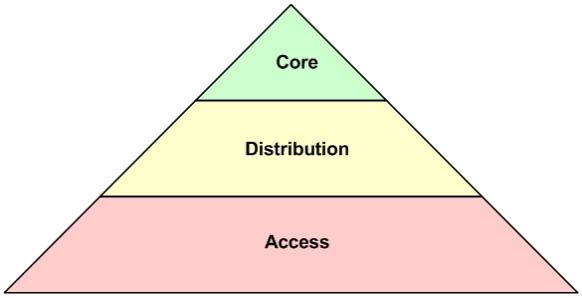

Figure 2.0.3a

STABILITY PRINCIPLE:

To ensure stability of the network transport layer, three principles are recommended:

1. Single vendor routers will be used exclusively within the network
2. The State of Montana Intranet will be managed from a central entity
3. The high-speed core network layer will be fully redundant

The use of single vendor routers exclusively, simplifies configuration control and allows for a proactive approach to router monitoring and management. This also leverages the existing IT investment and personnel resources, often referred to as soft dollar cost.

Managing the State's Intranet from a central entity simplifies change management and allows for consistency within daily network operations.

Having the high-speed network core layer fully redundant improves availability and fault tolerance of the network infrastructure.

SCALABILITY PRINCIPLE:

This design allows true scalability and flexibility into the design with two basic principles:

1. Exclusive use of single vendor routers within SummitNet. The routers support a full range of transport media employed in the State of Montana's network. Upgrading bandwidth or adding functionality is a simple hardware upgrade rather than replacement.

2. The hierarchical topology design transparently accommodates staged injection of new technology. It accepts additional functionality at any layer without affecting other layers, and provides the design structure to scale the State of Montana network.

SECURITY PRINCIPLE:

Stateful firewalls placed strategically throughout the network enforce the State of Montana's network security policies. These firewalls are placed at access points into the State of Montana network, primarily at the access Layer. In order to maintain the core's key function as a high-speed transport mechanism, there will be no firewalls in the core of the network. The two security principles are:

1. Ensure that only authorized users access State resources

2. Protect the State of Montana network from unsecured users and malicious activity from the Internet

Additionally, network devices whether printer, laptops or desktops must be authenticated prior to admittance to the network.

2.0.4 MODEL

SummitNet's core layer has two 20Mb ATM PVC paths for diversity today. One path is via Great Falls; the other path is via Bozeman connecting Helena to Billings. The purpose of the core layer is to address inter Local Access and Transport Area (LATA) boundary issues and provide high-speed bandwidth between the distribution layer locations. There are two aggregation routers, one in Billings, and one in Helena.

An illustration of SummitNet is shown in Figure 2.0.4a.

VIEW OF SUMMITNET NETWORK

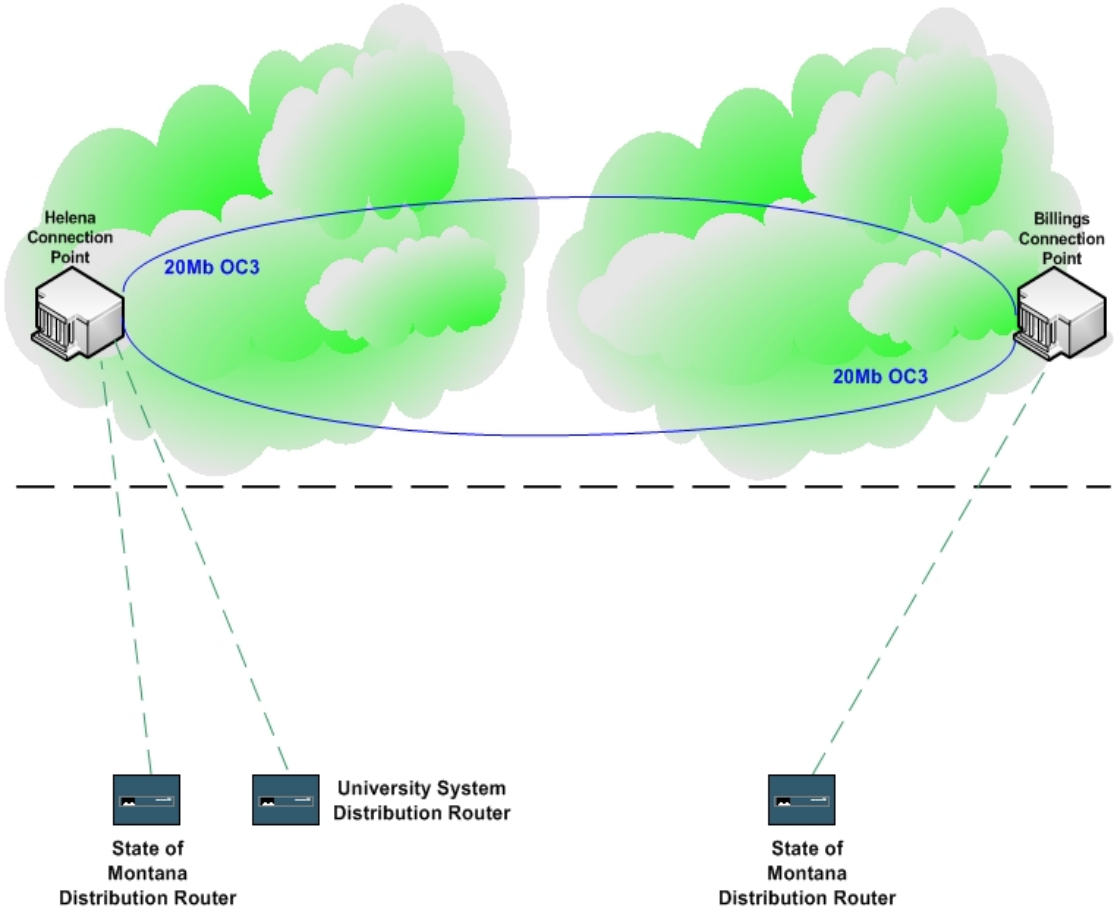

Figure 2.0.4a

SummitNet's distribution layer locations, Helena and Billings, are the primary aggregation points for the State's WAN circuits based on eastern and western LATA boundaries. The State's WAN circuits are comprised of the WAN connections described in the access layer. The distribution layer locations, Libby, Lewistown, and Sidney aggregate WAN circuits in the corresponding town onto a shared circuit(s) delivered into the primary distribution layer locations in Helena or Billings. These locations were installed to increase bandwidth to the agency sites located in these towns and minimize the duplication of carrier mileage charges.

The access layer is the first connection point onto SummitNet for most State users. The connection is DDS point-to-point, frame-relay, or DSL. These are transported via ATM PVC's into the primary distribution layer locations in Helena or Billings. An illustration of the State's Network is shown in Figure 2.0.4b.

VIEW OF THE GOVERNMENT NETWORK

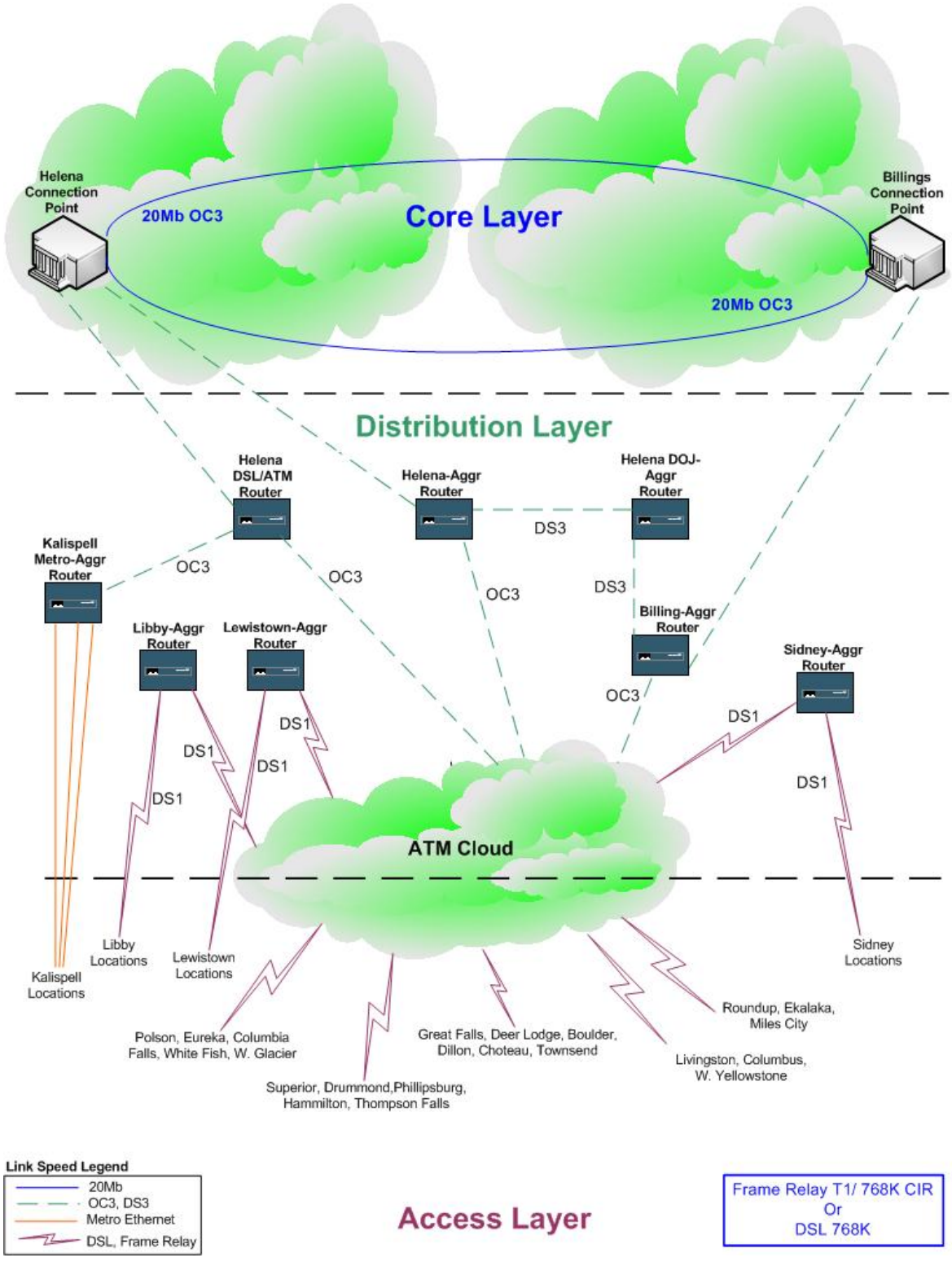

Figure 2.0.4b

Montana's University System network utilizes SummitNet as its core also. The University System is logically separated from the State's side of SummitNet. There is a connection point at Helena into to the State side of the network and its resources.

The University System distribution layer locations in Helena, Bozeman, and Missoula are the primary aggregation points for voice and data WAN circuits. Distribution layer circuits are comprised of ATM PVC's that are delivered into the SummitNet core at Helena.

The University System access layer is the first connection point into SummitNet for all university campus locations. The access layer circuits are frame-relay, ATM, or DS1 Circuit Emulation (CE, used for voice). There are 14 DS1 Circuit Emulation connections for voice transport to the various university and State agency locations. The Circuit Emulation is used for voice and video. The Montana University System Network is shown in Figure 2.0.4c.

VIEW OF THE MONTANA UNIVERSITY SYSTEM NETWORK

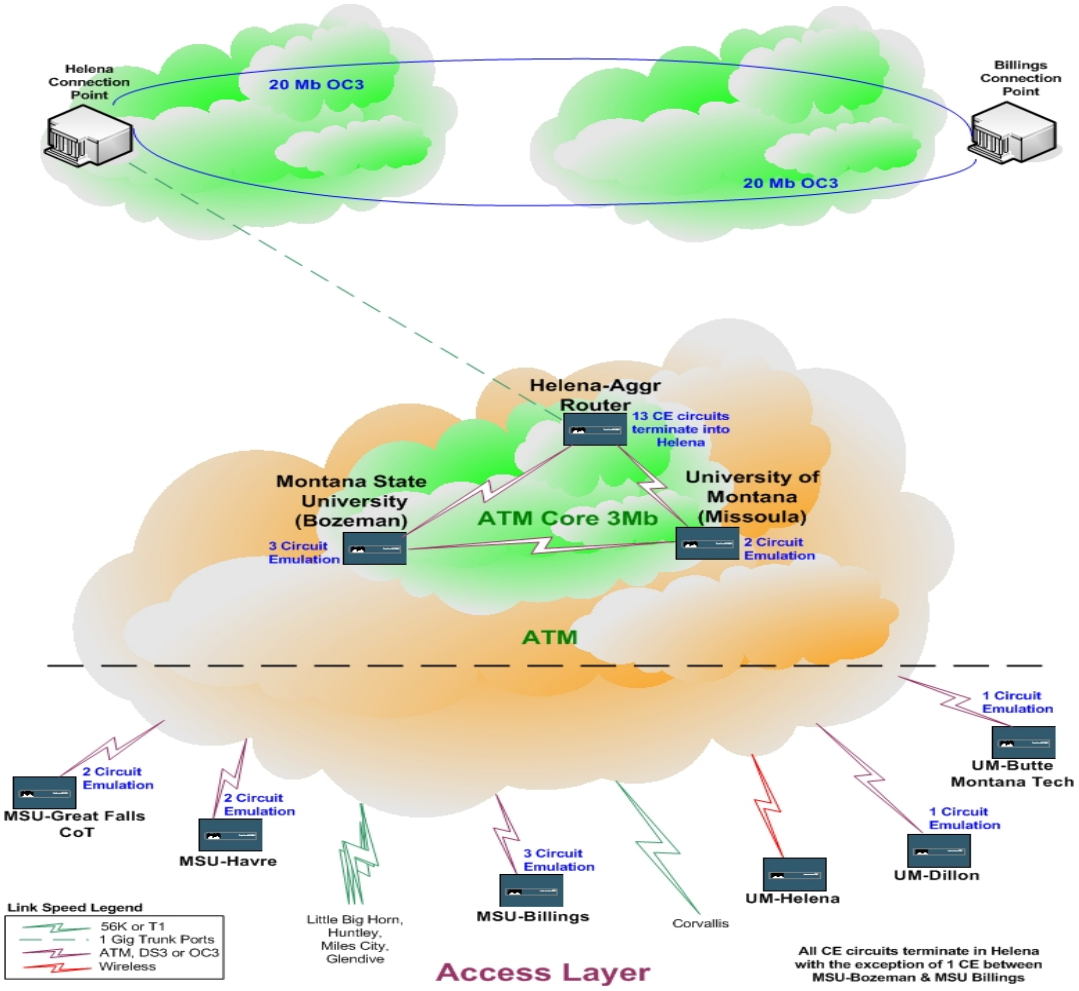

Figure 2.0.4c

Scalability is one of the most important design issues. If the network is scalable, it is easy to expand, maintain, and troubleshoot. The network transport model achieves scalability by compartmentalizing functionality. The compartmentalization is accomplished with the hierarchical network architecture as outlined in Network Transport section 2.0.3. With a hierarchical network, both scalability and stability are easily achieved.

The University System is contained in a separate compartment (or layer) from the State side of the network. These two compartments combined together comprise SummitNet. In other words, the University and the State system are logically separated.

The proposed model in Figure 2.0.4d provides for a fully redundant and diverse core to transport the information as fast and reliably as possible. The distribution layer allows for inter-connecting any type of remote facility and automatic failover between distribution points thus accomplishing the goal of moving data around SummitNet and scaling of the Intranet. The access layer allows for inter-connecting users to the network.

The proposed design model for the State encompasses all four of the network transport design principles as shown in Figure 2.0.4d.

PROPOSED NETWORK TRANSPORT MODEL

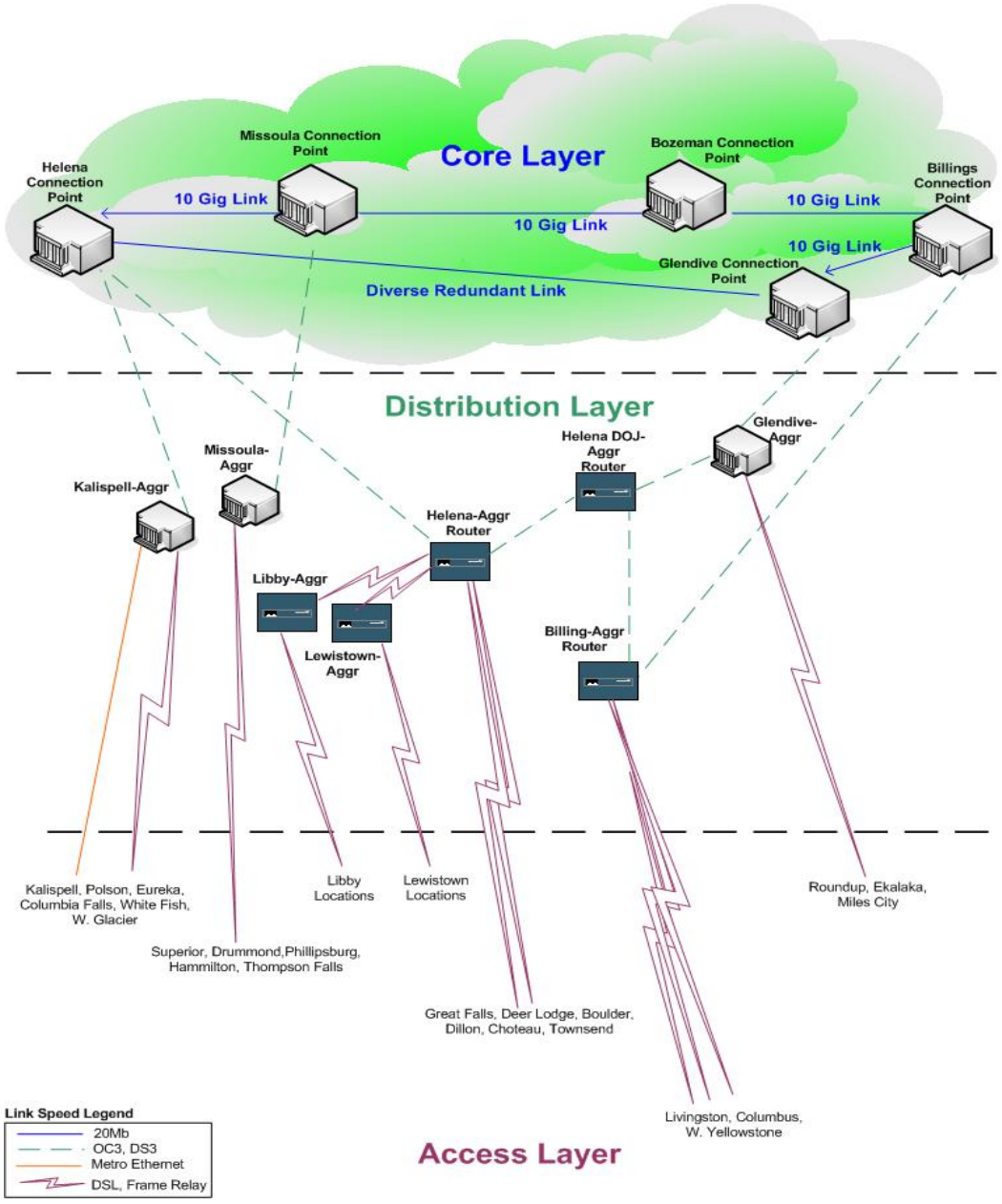

Figure 2.0.4d

The Security for the proposed model is based on the concept of compartmentalizing network services and assigning levels of trust. The idea is that the normal user does not need access to all services within the network. By compartmentalizing network services and assigning these services levels of trust, users are allowed to access only those services they need to perform their duties. As an example, a State Fund user does not need to access the Dept. of Revenue's (DOR) property tax database.

Non-Trusted Networks consist of any network or connection that is not part of the State of Montana core network (agency, counties, cities, and Internet connections). These networks are allowed access to the compartmentalized areas of the secured network via a firewall or a firewall feature set on a router.

SECURITY RING MODEL

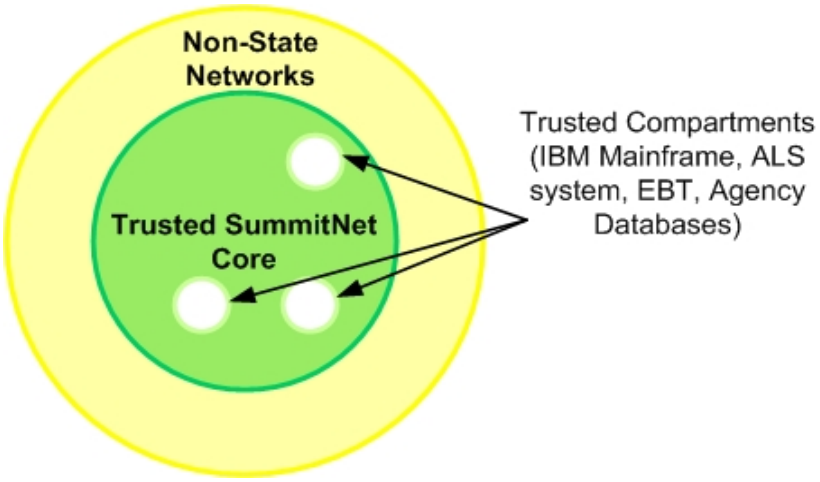

Figure 2.0.4e

The network is only as secure as the least secured device. It is the desire of the State to both authenticate each device and ensure adequate security patches are applied to each device. These activities are performed prior to the device being allowed to communicate on the network.

2.1 HIGH SPEED CORE NETWORK

As the network expands from a best effort network to a predictable, reliable, and redundant high-speed network, a reliable core transport between services centers and to the Internet is required. The services centers currently exist in Helena and Billings.

While there are two ATM circuits between Helena and Billings, only secured SummitNet data is transferred between them. Due to carrier limitation, these circuits cannot be expanded in size to include services such as Unified Messaging (voice, video), DMZ, or Internet.

It is the intention of the State to acquire a private core network. This core network would diversely exist between Missoula and Glendive with drop and insert points along the way. The drop and insert points would allow easy access for remote locations.

2.1.1 GOALS

The goal is to build a high speed, predictable, reliable, and redundant core network between services centers that can transport both unsecured (Internet/ DMZ) traffic as well as secured traffic.

2.1.2 ISSUES AND CONCERNS

The primary issue is one of funding. The new core transport network is expected to cost $3,200,000.00. The State Legislature must fund this project.

The core network transport is the foundation for the strategic plan. If the new core transport network is not funded, all other aspects of the plan are jeopardized.

2.1.3 PRINCIPLES

To obtain these goals, the following principles are proposed:

1. ITSD manages the system
2. The State of Montana and University System participate fully
3. Single vendor equipment is used exclusively
4. The core transport network terminates in Spokane to accommodate Internet access for the University System

1. ITSD MANAGES THE SYSTEM

The State of Montana currently manages all aspects of the network transport except layer 1 of the OSI model (the physical layer or the actual cable and its signal). Typically the carrier is responsible for layer 1. In order to deliver a reliable and predictable network transport service, ITSD proposes to manage layer 1.

2. THE STATE OF MONTANA AND UNIVERSITY SYSTEM PARTICIPATES FULLY

The State of Montana and the University System intend to participate fully in all aspects of the core network transport. A consortium called Northern Tier has been organized for this purpose.

3. SINGLE VENDOR EQUIPMENT IS USED EXCLUSIVELY

The State of Montana and the University System use single vendor network equipment exclusively. This allows for easy installation and troubleshooting.

4. THE CORE TRANSPORT NETWORK TERMINATES IN SPOKANE TO ACCOMMODATE INTERNET ACCESS FOR THE UNIVERSITY SYSTEM

The University System transports large amounts of data to the research Internet2 (I2) and the commodity Internet (Internet). This requires a direct connection to the Northwestern GIGAPOP in Spokane, WA.

2.1.4 MODEL

The core network transport model encompasses all four of the design principles. The models are:

1. ITSD MANAGES THE SYSTEM

ITSD proposes to oversee the management of the entire core network transport system.

2. THE STATE OF MONTANA AND UNIVERSITY SYSTEM PARTICIPATE FULLY

The State and University System participate fully in every aspect of the core network transport system.

3. SINGLE VENDOR EQUIPMENT IS USED EXCLUSIVELY

A single vendor optical product line is being used for the Dense Wave Division Multiplexing (DWDM) aspects of this network. Single vendor routers are being used for POP aggregation into the DWDM system, and IPS (Intrusion Prevention System) is being used for inspection of the data prior to admittance to SummitNet.

4. THE CORE TRANSPORT NETWORK TERMINATES IN SPOKANE TO ACCOMMODATE INTERNET ACCESS FOR THE UNIVERSITY SYSTEM

A connection point from Missoula to Spokane allows for a hand off of commodity and Internet2 traffic.

The model proposed is a Dense Wave Division Multiplexing (DWDM) system. DWDM operates on a single fiber pair, and lights different wavelengths. The DWDM system allows for 32 different or independent light waves of 10 Gigabit Ethernet each. The system proposed is comprised of two 10 Gigabit Ethernet (Gig) links from Missoula to Glendive. One 10 Gig link is for the use of the State of Montana, the other link is for the University System. Each link is designed with a N+1 system. N+1 is a hot standby card in each chassis at every location for automatic failover in the event of a card failure anywhere along the line. While N+1 offers redundancy, it does not offer diversity.

Since this entire system operates on a single fiber pair, if the fiber failed, or was cut, service does not continue. Diversity is offered by the two diverse links shown in Figure 2.1.4a. These links connect Helena to Billings through a northern route, and Helena to Missoula through Kalispell.

CORE TRANSPORT MODEL

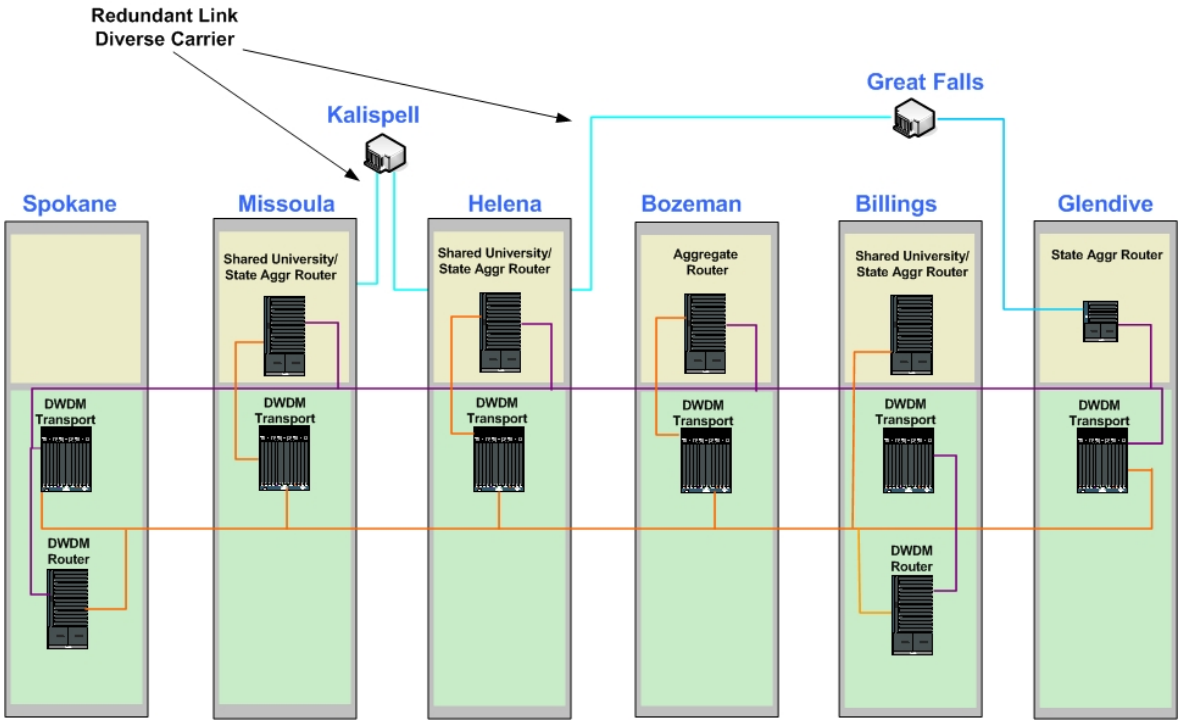

Figure 2.1.4a

2.2 NEW SERVICES CENTERS

Today the Mitchell building in Helena houses the main services center for the State of Montana. This location is the access point for all services coming in from the WAN and Internet. The majority of the services for the State are located in this building.

There are three main issues with the Mitchell building:

1. Difficult to secure
2. Vulnerable to natural disasters
3. Space constraints

Additionally there are approximately 15 individual "data centers" in the Helena area independently operated by different State agencies. These data centers have varying levels of security, HVAC, diversity, and redundancy.

To address these issues two new Services Centers are proposed to house systems for unified messaging, traditional voice, and data systems.

The Services Centers will be large enough to accommodate capacity requirements of ITSD and agencies currently operating independent data centers as well as anticipated growth.

2.2.1 GOALS

The four goals of the Services Centers are:

1. Continuity of Government
2. Improved Services
3. Security
4. Efficiency of Government Services

The two Services Centers are to be located at least 250 miles apart. This is the minimum recommended distance for industry best practices to implement services centers.

In the event of a disaster these Services Centers will be far enough apart that the second Services Center will not be affected by the event and can continue to operate. If one of the Services Centers goes down either for maintenance, or unexpectedly the second Services Center continues to function. This allows for continuity of government. These two Services Centers will be both active and able to function independently. These items combined result in improved services.

Since these Services Centers are designed from the ground up with security in mind, all aspects of security best practices, both physical and systems/network, are implemented in the best interest of the State.

These two Services Centers are able to house all services required for the State of Montana to operate. This allows for the elimination of the smaller data centers around the state thus increasing the efficiency of the State services.

These four goals achieve the overall goal of improved government services not only for its internal operations, but also for the University System, Local Government, and the citizens of the State of Montana.

2.2.2 ISSUES AND CONCERNS

The two issues and concerns are:

1. Cost
2. A new way of doing business for State government

The cost of the facility will need to be approved by the State Legislature. The procurement and allocation of the funds is a large undertaking.

Today many State agencies have their own data center. To begin handling these services out of a single location is a new way of conducting business for these agencies.

2.2.3 PRINCIPLES

The principles for the new Services Centers are:

1. Ability to leverage the Services Centers for disaster recovery
2. Ability to continue operations in the event of a planned or un-planned outage
3. Ability to load balance the services provided

2.2.4 MODEL

Two Services Centers are being proposed. One in Helena, and one located in eastern Montana. These Services Centers are not primary and failover; rather they are both fully functional active/active Services Centers. If one of the Services Centers fails, the second one continues to function. This allows for continuity of business in the event one of the Services Centers fails.

The two facilities must be far enough apart so as not to be impacted by the same natural disaster (i.e. earthquake, or storms resulting in loss of power).

Since these two Services Centers are active at all times they can load balance services.

These facilities are to be built modular in fashion, to facilitate easy expansion.

These two new Services Centers are being proposed to the State Legislature during the 2007 session, with expected completion in the winter of 2009/spring of 2010.

2.3 AGGREGATION POINTS-OF PRESENCE (POP)

Today there is an aggregation Point-of Presence (POP) in Helena and Billings. These POPs aggregate the agency WAN locations by LATA. The eastern LATA terminates into Billings, and the western LATA terminates into Helena. These connections are not redundant. If the eastern POP fails, the western POP does not take over the transporting of data.

The State also pays mileage charges from the remote connection back to the POP. In an effort to reduce the mileage charges and make the WAN more redundant a new WAN aggregation design is needed.

2.3.1 GOALS

The five goals of the aggregation POPs are:

1. Support Quality of Service (QoS) end to end
2. Secure
3. Easy to scale and implement
4. Support automatic failover
5. Support regionalized services

2.3.2 ISSUES AND CONCERNS

There are two issues and concerns in being able to implement the stated goals. They are:

1. Ability to achieve scalability and automatic failover
2. Lack of inspection at the access layer

1. ABILITY TO ACHIEVE SCALABILITY AND AUTOMATIC FAILOVER

There are two methods of achieving the stated goals of scalability, and automatic failover. The first is the more traditional method of establishing additional POPs and leasing bandwidth and services to obtain automatic failover. This method has been used as industry best practices for a number of years but can get expensive.

Multiple POPs are required to establish distribution layer redundancy. In many instances, the remote location must purchase two or more connections, each terminating to a different POP. The remote location in many instances incurs the mileage charge twice if two links are needed. This method assumes a high-speed core network between Helena and Billings, which transports the re-routed data in the event of a failure.

The second method is a relatively new offering by the communications industry. This method called Multiprotocol Label Switching (MPLS) does not usually require more than one link to the remote office. The State is currently investigating this method and the communication companies offering the service. MPLS is not mileage sensitive and automatically chooses the optimal POP. A minimum of two POPs is required for this method.

2. LACK OF INSPECTION AT THE ACCESS LAYER

There are many State agencies, all with varying levels of patch management and virus protection. The traffic on the secured network does not require inspection through a firewall, but it should be inspected through an Intrusion Prevention System (IPS) to correlate events and detect traffic anomalies.

Industry best practice dictates this type of inspection is done prior to traffic being placed onto the secured network at the distribution layer. As such an IPS should be placed at the POP router. Today, the State uses Cisco's Security Monitoring Analysis and Response System (MARS) appliance for IPS. This system gathers and correlates data flow information from across the enterprise by means of strategically placed Cisco IPS devices. It uses our existing network and security investments to identify, isolate, and recommend precision removal of offending elements.

2.3.3 PRINCIPLES

The trend in the last several years for States is to install their own private high-speed core network and connect the remote locations through a POP. The POPs are managed by the individual States. The State of Montana intends to follow the same principle where possible. This allows the State to manage and grow the network more effectively and efficiently with minimal participation from outside entities such as communications vendors.

2.3.4 MODEL

The access layer places the traffic into a queue based on priority needs. The distribution layer transports the data based on this established queuing.

The aggregation Points-of-Presence model implements the model for transport as established in Network Transport section 2.0.4. The illustration of the aggregation points-of-presence model is shown in Figure 2.3.4a. With this model aggregation POPs can easily be added or removed as needed.

AGGREGATION POINTS OF PRESENCE MODEL

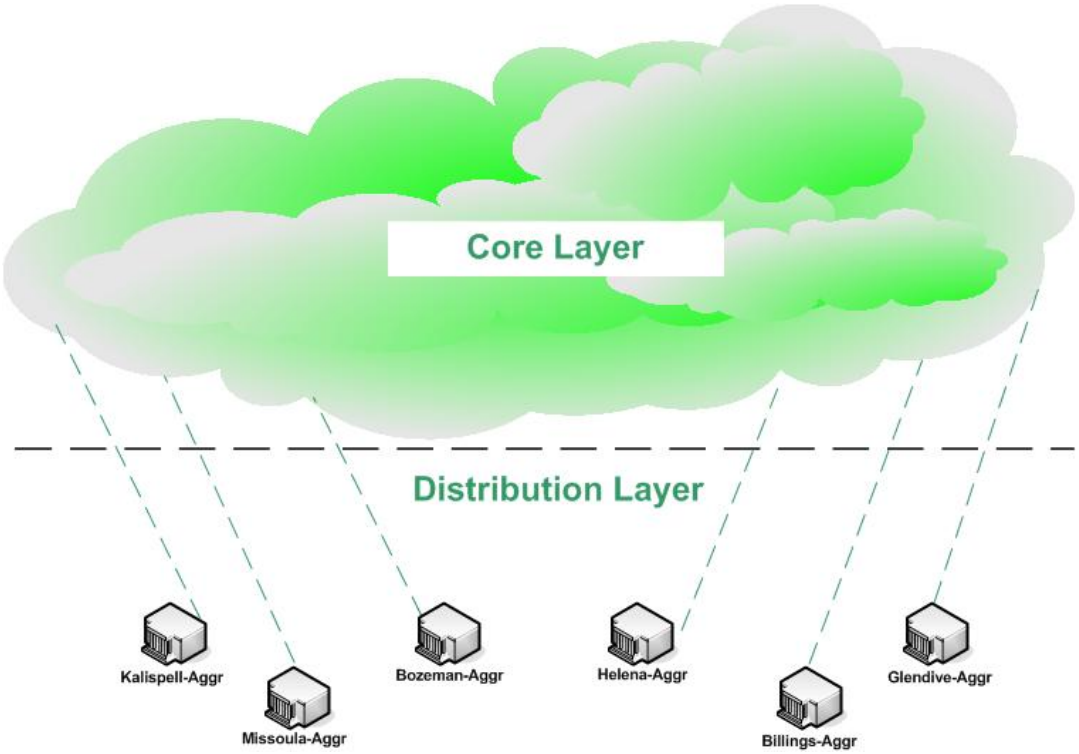

Figure 2.3.4a

2.4 INTERNET/ DMZ NETWORK

The State's Internet connection is provided by Visionnet and has an entry point in Helena and in Billings. Each location is front ended by a Cisco 3662 router and two sets of firewalls. This creates a DMZ where the Internet facing servers and external DNS are located. Figure 2.4a shows the Internet connections as they exist today.

CURRENT INTERNET/DMZ NETWORK

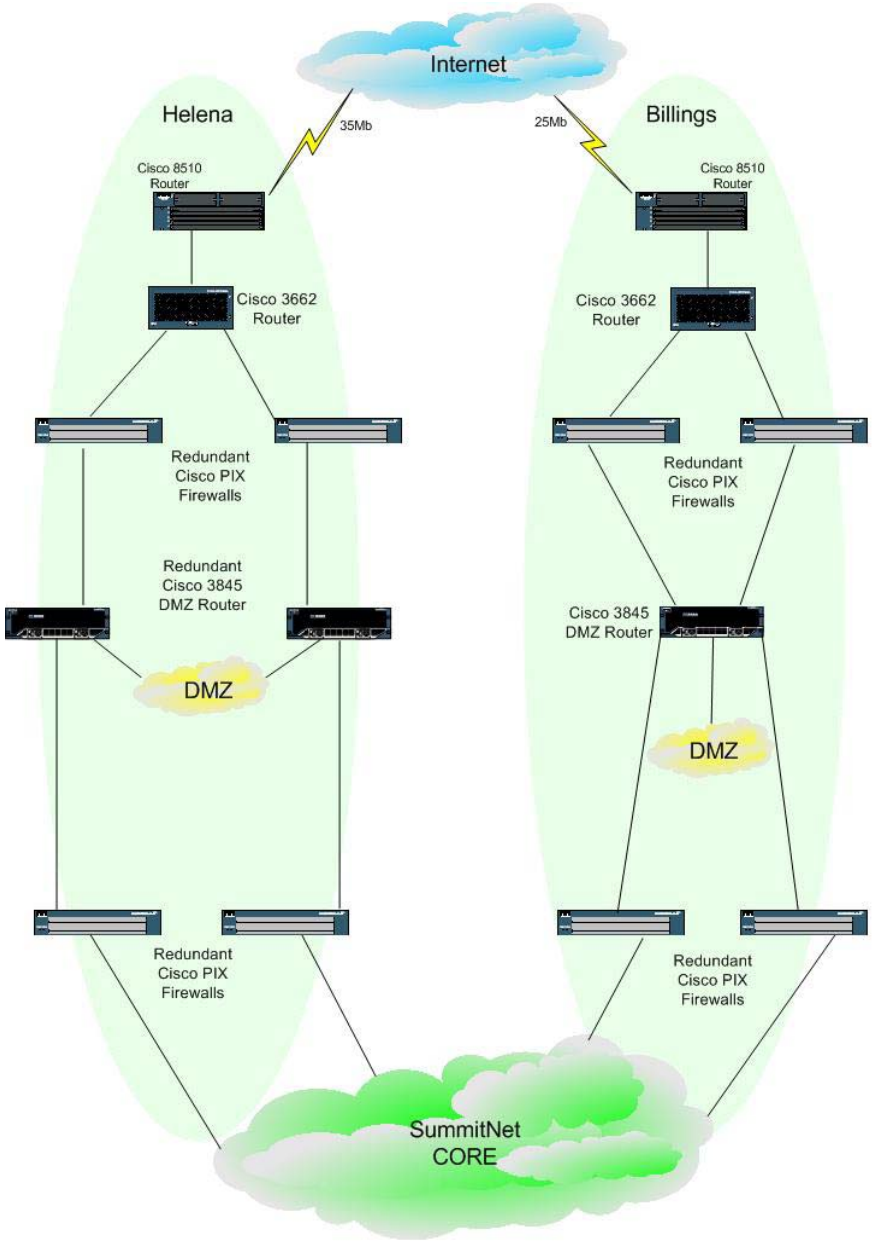

Figure 2.4a

The State users are divided geographically into a western LATA and an eastern LATA. All users accessing the Internet from the western LATA go out through the Helena connection. Users accessing the Internet from the eastern LATA go out through the Billings connection. All access into SummitNet from the Internet comes into Helena. If the Helena Internet is down, the traffic is re-routed into Billings. The flow of traffic is shown below in Figure 2.4b.

INTERNET TRAFFIC FLOW

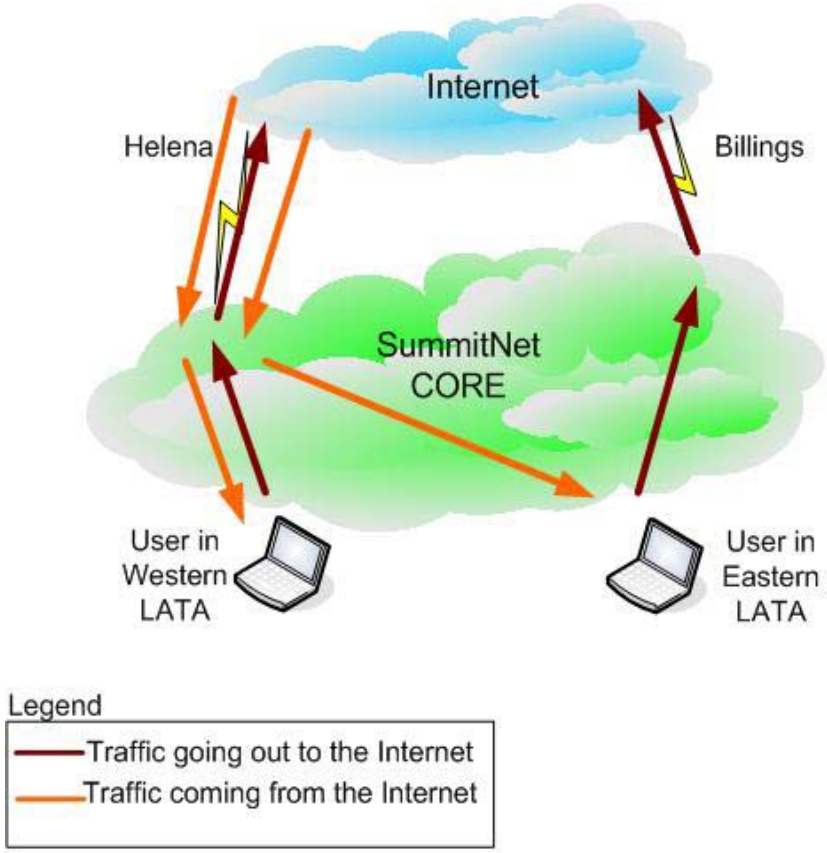

Figure 2.4b

2.4.1 GOALS

The goal of the DMZ is to provide an un-trusted network for SummitNet servers and services accessed by the public. The DMZ usually contains services such as Web servers, DNS servers, and Mail servers. In this way, the security of SummitNet is maintained by not allowing the general public into our trusted network, while at the same time providing the needed servers and services.

2.4.2 ISSUES & CONCERNS

There are four issues with the Internet/ DMZ:

1. Single Internet Service Provider (ISP)
2. DMZ extended throughout Helena
3. DMZ access extended to City/Counties
4. No traffic shaping of traffic to the Internet

1. SINGLE INTERNET SERVICE PROVIDER (ISP)

Today our Internet connection is terminated in two locations, but to a single Internet Service Provider (ISP), Visionnet. Having only a single ISP could potentially create problems for the State of Montana users accessing the Internet if the ISP experiences issues.

2. DMZ EXTENDED THROUGHOUT HELENA

The DMZ is an un-trusted network and should not come into contact with the trusted network (SummitNet), except through a firewall. The extension of the DMZ has been accomplished by transporting the DMZ virtual VLAN (Virtual Local Area Network), which is an un-trusted network, over the trusted network. Although logically these two networks are separate, they are physically traversing the same media.

The DMZ network is extended from the Mitchell building in Helena to almost every agency in Helena both on campus and off.

Figure 2.4.2a is an illustration of the agencies within Helena, which have extended DMZ networks.

DMZ NETWORK EXTENDED AREAS

Figure 2.4.2a

In addition, when a remote agency has a server that needs to communicate to the Internet directly such as Mail server, or Web server, a hole is punched in the firewall allowing this traffic through.

This results in a two-fold issue:

1. Un-trusted traffic traversing our trusted network
2. If a single server on the trusted network is compromised it could potentially infect any number of other trusted servers and ultimately bring down the State of Montana's network and services.

The practice of extending the DMZ to campus buildings, and punching holes in the firewalls to accommodate Internet facing servers within SummitNet has made it extremely difficult to secure, which in turn makes it difficult to manage.

3. DMZ ACCESS EXTENDED TO CITY/COUNTIES

When a city or county uses SummitNet to access the Internet, it is a common practice to punch a hole in the firewall so a city/country device such as a mail server can communicate directly with the Internet. SummitNet cannot guarantee the integrity of the server regarding software patch levels. Because the server is directly on SummitNet, its traffic is not inspected through a firewall, and it has the potential to compromise the integrity of SummitNet.

4. NO TRAFFIC SHAPING OF TRAFFIC TO THE INTERNET

Today there is no rate limiting or traffic shaping on the sessions going to the Internet. Currently the State leases 35Mb of bandwidth to the Internet. If a user sets up a peer-to-peer network for music download, or starts a large file download such as a virus software update, there is no limit on how much of the available bandwidth a single user can consume in a single session. The user can consume all available bandwidth up to the maximum of 35Mb. This impedes performance on mission critical applications that are essential to State government business.

2.4.3 PRINCIPLES

The primary objective of the DMZ is to provide an un-trusted network for SummitNet servers and services that are separated both logically and physically from the trusted SummitNet network by firewalls.

The second objective of the DMZ is to provide an un-trusted network for all non-State entities. These un-trusted entities are removed from the trusted SummitNet network thus reducing the size of the trusted network making it easier to secure, and manage.

2.4.4 MODELS

The three Internet/DMZ models to address the issues and concerns while honoring DMZ principles are:

1. Dual ISP
2. Condense the DMZ
3. Traffic shaping of traffic to the Internet

1. DUAL ISP

As the Internet begins playing a more prominent role in the State of Montana's day-to-day operations, it may be prudent to replace the Internet provider in Billings with an alternate Internet provider (ISP). When this occurs, it becomes necessary to run an External Gateway Protocol such as eBGP IV to allow automatic failover between the ISPs.

2. CONDENSE THE DMZ

Eliminating extensions of the DMZ to buildings within the Capitol Complex will reduce the size of the trusted network making it more secure and easier to manage. In the case of an Agency, City, or County this can be accomplished by either an IPSec tunnel from the un-trusted servers at the agency locations directly to the DMZ, or by placing these servers directly in the DMZ located in the Helena or Billings Services Center.

Today the DMZ is logically and physically separated between Helena and Billings. The new model, while physically separated, is now treated logically as one DMZ. This allows the services to be accessed from the Internet connection in Helena or Billings.

If a City or County requires direct access to the Internet for a server, the best solution is to place the server directly onto the DMZ either in the Helena or Billings. The following Network Transport section 2.5, Non-State Entity Access discusses this model. Until section 2.5 is implemented, an IPSec tunnel should be established from the City/County router directly to the Internet firewall. This eliminates the passing of non-State Internet traffic directly onto SummitNet.

4. TRAFFIC SHAPING OF TRAFFIC TO THE INTERNET

With a rate-limiting appliance, each session, based on user, IP address range, or type of traffic, can be regulated to control the amount of bandwidth consumed. It is expected when rate limiting is implemented on a per user basis, abuse of the Internet will dwindle since the individual user is no longer able to procure large chunks of the Internet bandwidth for their personal use.

Figure 2.4.4a shows an illustration of the proposed Internet connection model.

PROPOSED INTERNET CONNECTION MODEL

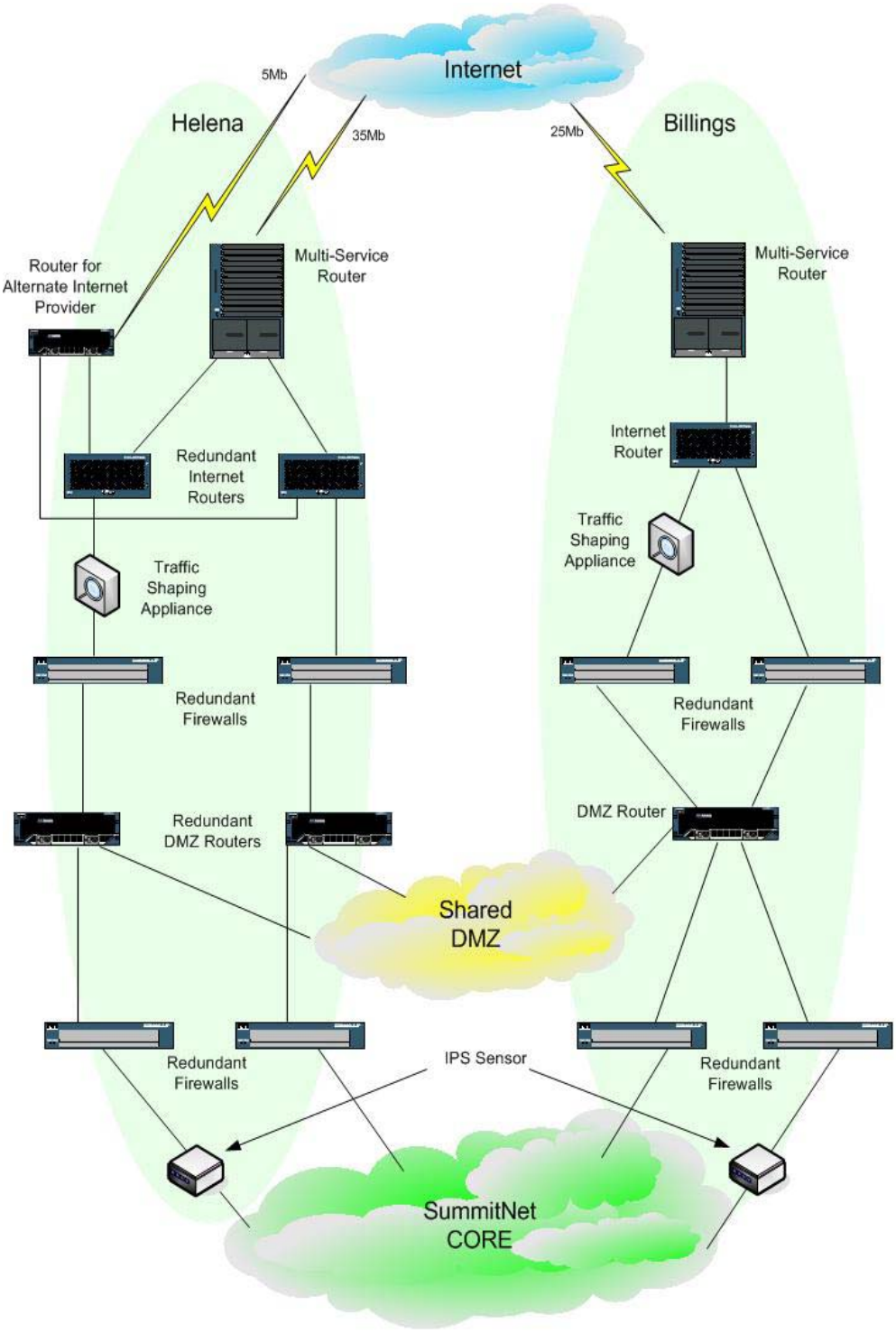

Figure 2.4.4a

2.5 NON-STATE ENTITY ACCESS

A sound security plan for implementing secured networks is to keep the secured network as small as possible. This is accomplished by placing all non-State managed devices in a DMZ outside of SummitNet. SummitNet is the secured entity.

Today all non-State agencies such as Cities and Counties are placed directly into SummitNet at the access layer. Figure 2.5a shows the City/County connecting at the access layer directly into SummitNet.

CITY/COUNTY CONNECTING INTO SUMMITNET AT THE ACCESS LAYER

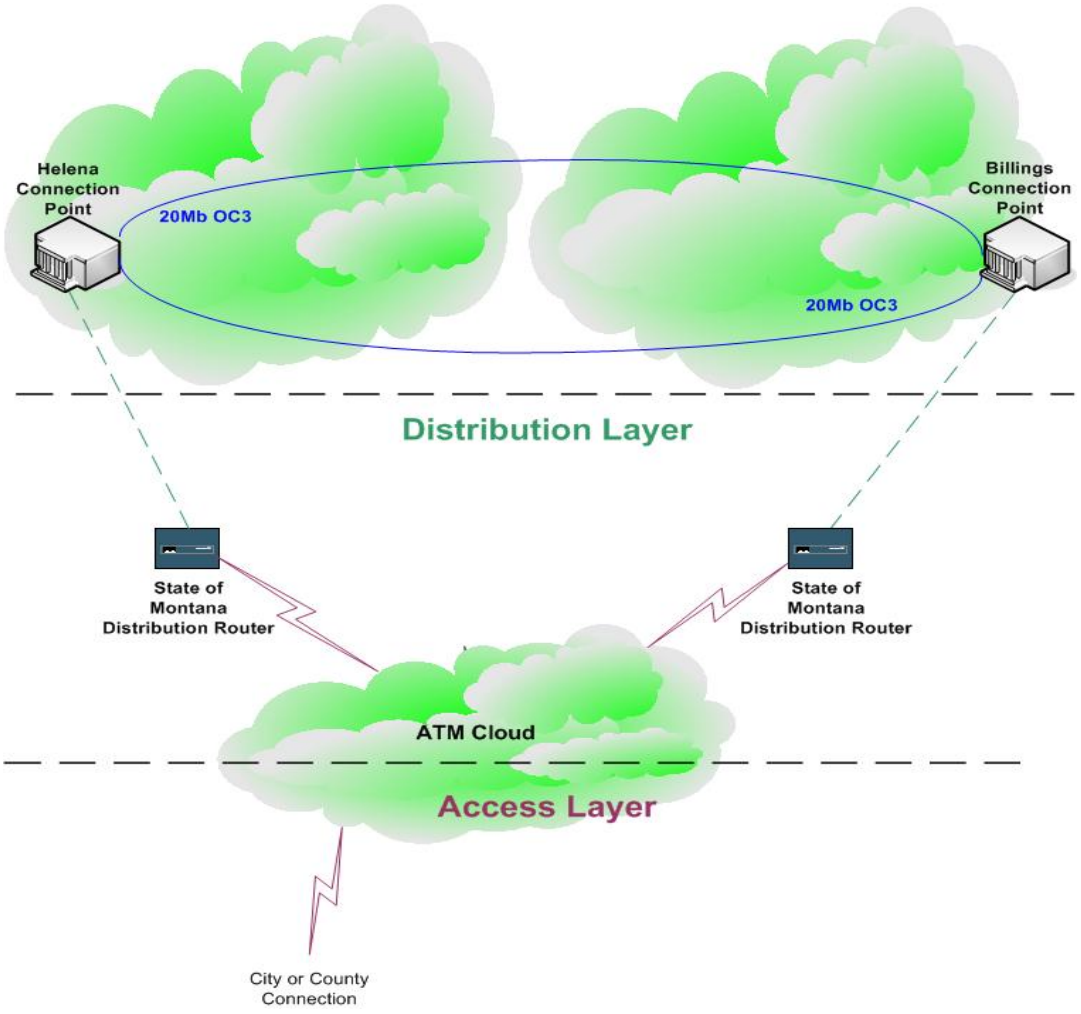

Figure 2.5a

As discussed previously if a City or County has a server that needs to communicate with the Internet such as a mail server, a hole is simply punched through the Internet facing firewall allowing the server direct access to the Internet. This poses a large security risk. Since the State of

Montana does not control this server, the patches or security level of the server cannot be guaranteed. If the server is on the secured network, and the server is compromised, SummitNet is compromised. This places SummitNet at risk due to the fact that the secured network does not pass any traffic through a firewall to gain access to resources, such as State server farms or mainframe.

A more secure method of allowing non-State entities access to SummitNet is required. A DMZ for non-State entity access must be created.

The DMZ model consists of access for Cities, Counties, and State Vendors/Contractors. Looking forward, the DMZ model could also include K-12 Schools and School Districts. This connection model facilitates connections with dedicated circuits.

Entities with connections outside of SummitNet continue to access SummitNet DMZ resources through the Internet model.

2.5.1 GOALS

The goal of the non-State entity access is to provide a connection point where the traffic must pass through inspection such as a firewall before being allowed access to secured resources within SummitNet.

2.5.2 ISSUES & CONCERNS

While this method of quarantining non-inspected, non-secured traffic follows industry best practices, it is a new concept for the State of Montana.

Once this model is in place, there is considerable effort required to migrate the non-secured connections already connected to SummitNet to the Non-State Entity Access model.

2.5.3 PRINCIPLES

The objective of the non-State entity access DMZ model is to provide an un-trusted network for all City, County, Vendor/Contractor, and School connections to terminate into. These un-trusted entities are removed from the trusted SummitNet network thus reducing the size of the trusted network making it easier to manage and secure.

2.5.4 MODELS

The model for non-State entity access is a DMZ similar to the Internet DMZ. This DMZ sits parallel with the Internet DMZ and shares the DMZ router and Internet router.

This model provides access for entities such as Cities, Counties, Vendors/Contractors, or Schools. Figure 2.5.4a shows the proposed non-State entity access connection model.

PROPOSED NON-STATE ENTITY ACCESS CONNECTION MODEL

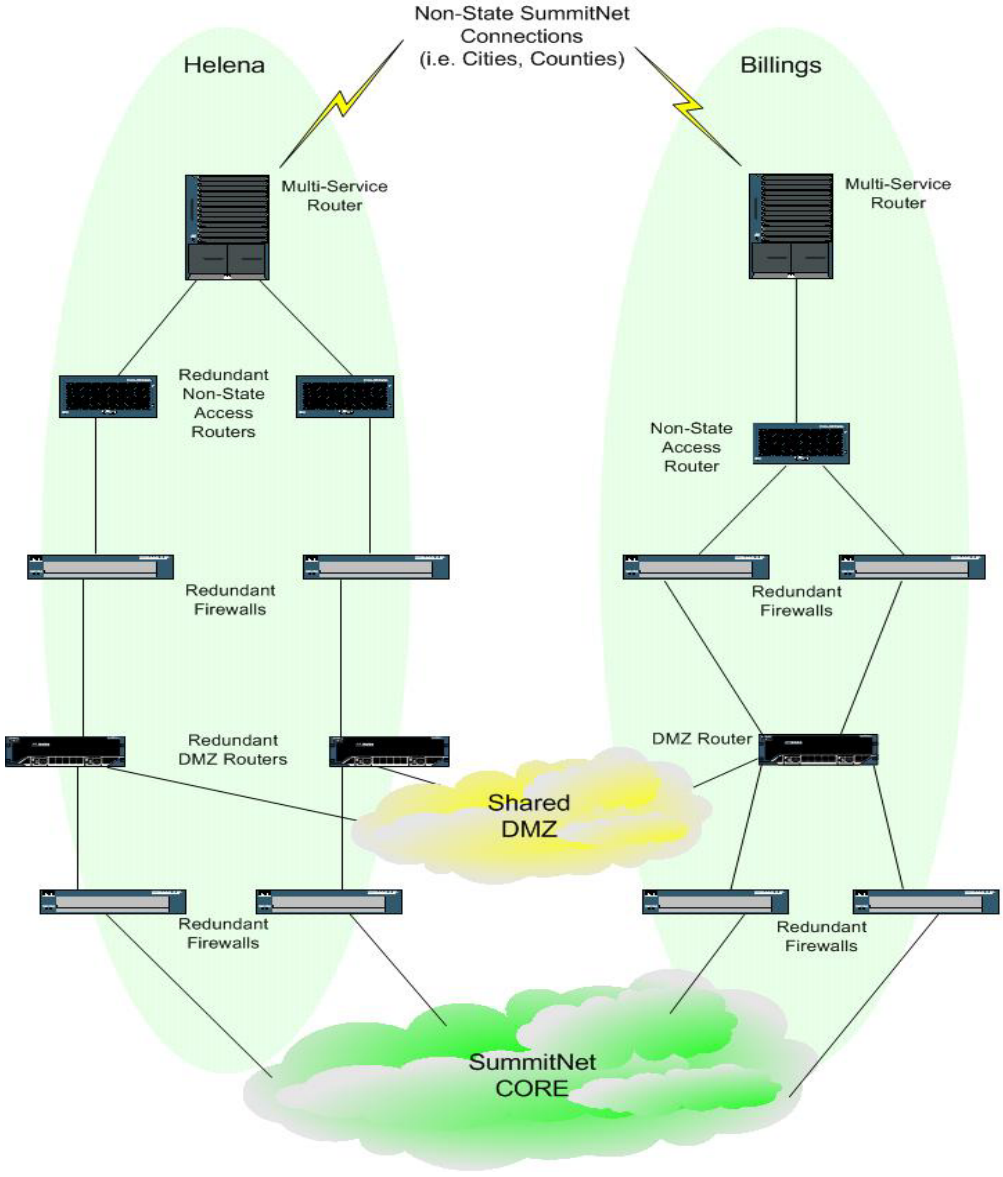

Figure 2.5.4a

2.6 CAPITOL COMPLEX UPGRADES

The Capitol complex upgrades are divided into two sections.

- Cable Plant Upgrades
- Network Equipment Upgrades

2.6.1 CABLE PLANT UPGRADES

The Capitol Complex has fiber optic connectivity between the buildings. The fiber is all multimode 62.5/125mm laid out in a ring fashion. There are 24 strands of multimode to each building from the previous building. The fiber plant is over 15 years old and was originally designed for Token Ring architecture. In Token Ring architecture the first connection made is to building #1 (Mitchell building), which then has a fiber connection over to building #2, then a connection from building #2 to building #3 and so on and so on, until a connection is run from the last building back to building #1, creating a ring.

Since Token Ring architecture ran at either 4Mb or 16Mb and ran from building to building multimode fiber was adequate.

The network has since been replaced with Ethernet, which is logically a bus technology arrayed in a star. Star topology requires the fiber from any building be run directly back to the hub, which is the Mitchell building. The distance from the buildings back to the Mitchell building is at the limit or exceeds the supported distance for Gigabit Ethernet over Multimode in some instances. Multimode fiber only supports Gigabit Ethernet (1000Mb) over short distances (usually less than 550 meters).

Due to distance limitations, the Ethernet network connections between the campus buildings are sometimes patched together from building to building to achieve 1000Mb (Gig) speeds. There is also limited redundancy between the buildings.

Desktops and servers within the Capitol complex are routinely connected at 1000Mb speeds. If access devices are running at Gigabit Ethernet speeds, the uplink between buildings must be scaled to handle the additional capacity.

Figure 2.6.1a shows the fiber plant as it exists today.

EXISTING FIBER PLANT

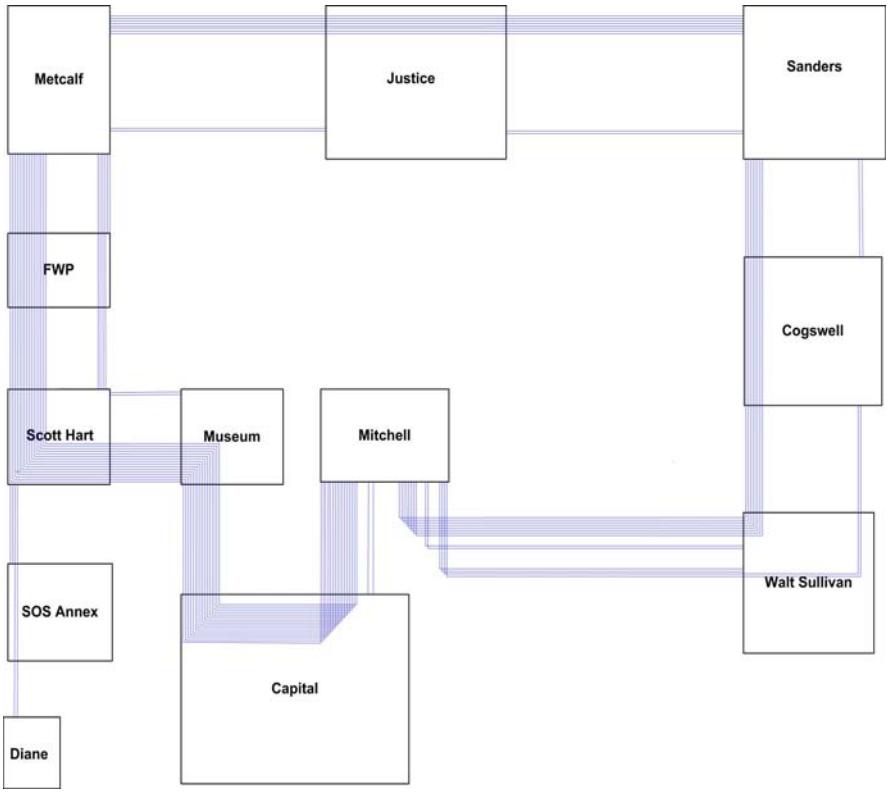

Figure 2.6.1a

A new fiber plant is needed to resolve the above-mentioned issues.

2.6.1.1 GOALS

The goal of the new fiber plant is to be able to offer various technologies between the buildings on the Capitol complex in a highly available, fault tolerant manner.

The proposed fiber plant supports these technologies:

- Gigabit Ethernet (10,000Mb or 40,000Mb)
- SONET
- Extended Fiber Channel
- DWDM

2.6.1.2 ISSUES AND CONCERNS

There are four issues and concerns with the existing fiber plant:

1. The Ethernet network connections between the campus buildings are patched together to achieve 1000Mb (Gig) speeds.
2. Limited redundancy between buildings.
3. It is not possible to increase the speed between the buildings using multimode fiber.
4. Unable to offer converged technologies between the buildings due to the lack of extra fiber pairs between buildings.

2.6.1.3 PRINCIPLES

The principle of the cable plant upgrade is to provide star topology using single mode fiber.

2.6.1.4 MODEL

The model for the cable plant upgrade is to install 24 strands of single mode fiber from each building on the upper campus to the Mitchell or Metcalf buildings. This provides enough fiber capacity to meet the needs for the State of Montana's Intranet for the next 10 years.

PROPOSED ADDITIONS TO THE FIBER PLANT

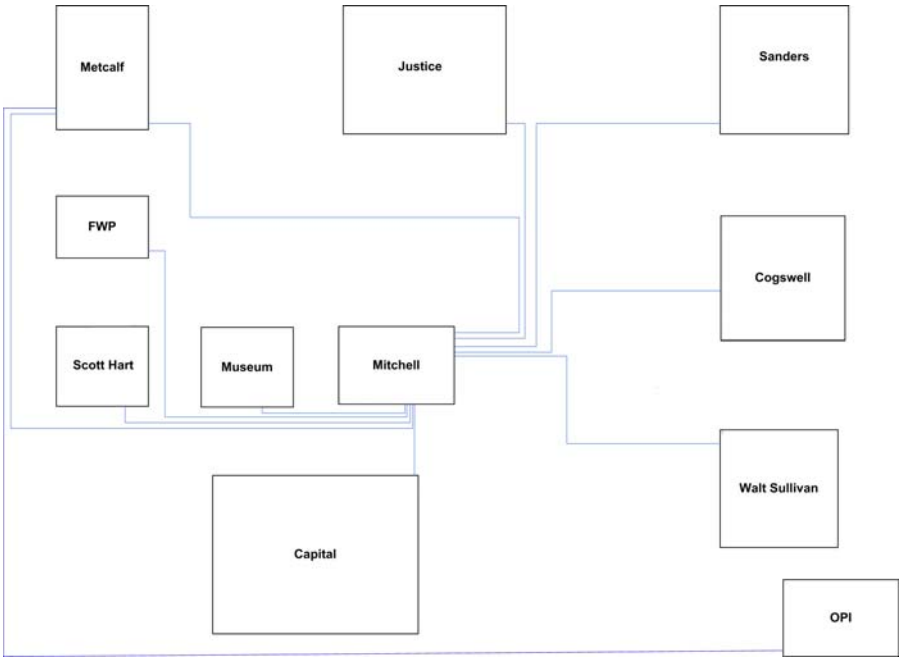

Figure 2.6.1.4a

While this model provides for redundancy at layers two and three of the OSI model (data link and network), layer 1 (physical) redundancy is not offered. This model does provide for two entry points into the Mitchell bldg. The proposed fiber plant utilizes the existing single entry into each building, with a single path back to the core network building(s).

2.6.2 NETWORK EQUIPMENT UPGRADES

The network within Helena, including the Capitol Complex is comprised of Cisco switching equipment. If the building has enough users it contains a 65xx platform switch with line cards of various flavors to facilitate user device connectivity such as desktops and printers. If these switches are on the Capitol Complex they are connected via a 1Gigabit Ethernet connection over multimode fiber. As mentioned earlier, this fiber is non-redundant and non-diverse in nature. As a result, the switching infrastructure is also non-redundant and non-diverse.

There are two issues with the existing switch supervisor modules:

1. They were purchased before Quality of Service (QoS) and 802.1X were fully supported features.
2. They do not support the newer cards such as line rate Gigabit Ethernet or 10 Gigabit Ethernet.

The switch power supplies are not large enough to fully support the newer Power Over Ethernet (POE) line cards.

As a result it is necessary to update all of the 65xx switches within the Capitol Complex. New supervisor modules, fan trays, power supplies, and UPSs are required. It is possible to re-use all existing line cards.

In smaller buildings not on the Capitol Complex the switch is a smaller unit such as a Cisco 3548 or 45xx model. Many of the switches do not support QoS or 802.1X and are no longer manufactured or supported by Cisco and must be replaced.

2.6.2.1 GOALS

The goal of this section is to have a networking infrastructure that supports the overall network strategic architecture goals as defined in Network Transport section 2.0.1. To accomplish these goals the infrastructure must be able to support QoS and 802.1X.

QoS is needed to perform traffic shaping by prioritizing traffic. This allows mission critical applications and time sensitive applications such as voice and video to have allocated dedicated priority bandwidth.

802.1X is a method of securely connecting network devices into the network. Today once a network port has been activated, any network device can be connected to the network. The device is not authenticated against a directory structure such as the Enterprise implementation of Microsoft's Active Directory. The wireless system is already using 802.1X for all secured access into SummitNet.

2.6.2.2 ISSUES AND CONCERNS

The biggest issue and concern with the infrastructure equipment within the Capitol Complex and Helena is the age of the equipment. Almost all of the smaller switches are no longer manufactured or supported by Cisco. The age of this equipment poses two problems:

1. Prone to failure
2. Do not support the newer features required to deliver a stable, secure, and scalable network as defined in Network Transport section 2.0.1.

2.6.2.3 PRINCIPLES

The design and infrastructure equipment must meet the principles of:

- Hierarchy
- Stability
- Security
- Scalability

as defined in Network Transport section 2.0.3.

2.6.2.4 MODEL

The model for the network equipment upgrades is a simple one; upgrade using single vendor switches and routers using features such as QoS, and 802.1X. A detailed parts list has been generated by location and submitted for allocation of funds. These upgrades are expected to commence in the FY '08 budget.

2.7 CONNECTION MODELS

The goal of this section is to develop a flexible model for each connection type. Bandwidth will be determined on a case-by-case basis as more detailed information about applications and organization structure becomes available.

The connection model section is divided into six areas:

1. State Agencies
2. University System
3. Local Government (City/ County)
4. K-12 Schools and School Districts
5. Vendors/ Contractors
6. Remote Access

These connection models connect to SummitNet either as secured or un-secured. If the model is considered secured, such as a State agency, the connection terminates into the POP routers and is placed directly into SummitNet without inspection through a firewall or router running firewall feature set. If the model is considered non-State, such as a school, or city/county, the connection terminates into a non-secured connection point.

There are two non-secured connection points into SummitNet, the Internet, and the non-State DMZ set up for non-State dedicated connections. If the non-State entity does not have a State provided dedicated connection; the connection terminates through the Internet just as regular Internet traffic does today. If the non-State entity terminates through a State provided dedicated circuit, the connection is made into the DMZ as described in Network Transport section 2.5.

Each connection model is discussed below with regards to security, and access needs.

2.7.1 STATE AGENCIES

State agencies are assumed to be trusted entities and are allowed directly into SummitNet without inspection through a firewall. These connections are typically connected to the closest POP.

State agencies have dedicated circuits from their remote location back to the POPs either in Helena or Billings. These circuits range in size from 56K to 3.08Mb. The circuit size is based on business application requirements.

These circuits are actively monitored with networking capacity trending tools. These tools determine bandwidth utilization and circuit congestion. When a circuit reaches 60% utilization for

10% of the time during business prime time (6:00am - 6:00pm MST), the circuit is noted for upgrade.

2.7.1.1 GOALS

The goal is to provide adequate bandwidth to all State government locations while maintaining the integrity of SummitNet.

2.7.1.2 ISSUES AND CONCERNS

Since ITSD does not participate in application testing prior to launching an application onto the network, bandwidth needs for remote locations cannot be predicted. This is due in part to the lack of a robust test environment and the lack of a policy prohibiting new applications onto the network without being fully monitored in a test environment. This results in bandwidth adjustments being reactionary in nature.

2.7.1.3 PRINCIPLES

The principle for State agency connections is to treat these connections as secured and terminate the connections directly into SummitNet.

2.7.1.4 MODEL

State agencies use the secured access model as described in Network Transport section 2.0.4. The agencies connect at the access layer. The model is shown again in Figure 2.7.1.4a

MODEL OF STATE AGENCIES CONNECTING TO SUMMITNET

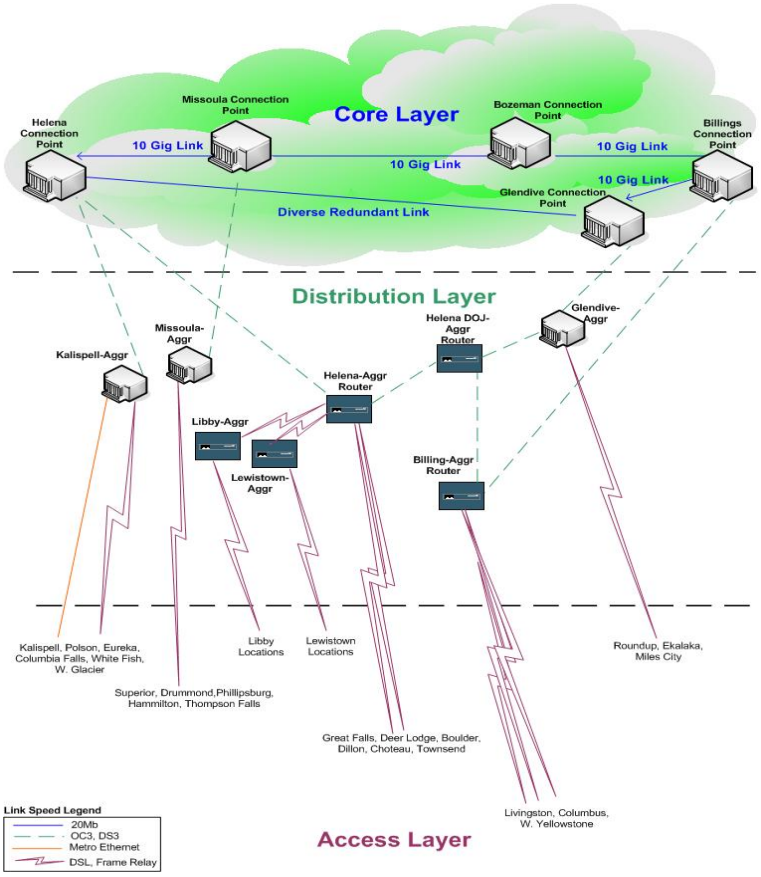

Figure 2.7.1.4a

2.7.2 UNIVERSITY SYSTEM

The University System share SummitNet resources at layer 1; that is the ATM cloud is a shared resource between the University System and the State of Montana.

2.7.2.1 GOALS

The goal is to provide a robust fault tolerant network while ensuring the separation of data at layer 2 and above.

2.7.2.2 ISSUES AND CONCERNS

There are no known issues or concerns at this time.

2.7.2.3 PRINCIPLES

The underlying principle of sharing resources at layer 1 is a proven concept that is working well for the University System and the State.

2.7.2.4 MODEL

Figure 2.7.2.4a illustrates the University System and how they connect to SummitNet for State resources. It should be noted that SummitNet does not transport the University System's Internet or Internet 2 traffic.

MODEL OF THE MONTANA UNIVERSITY SYSTEM CONNECTING TO SUMMITNET

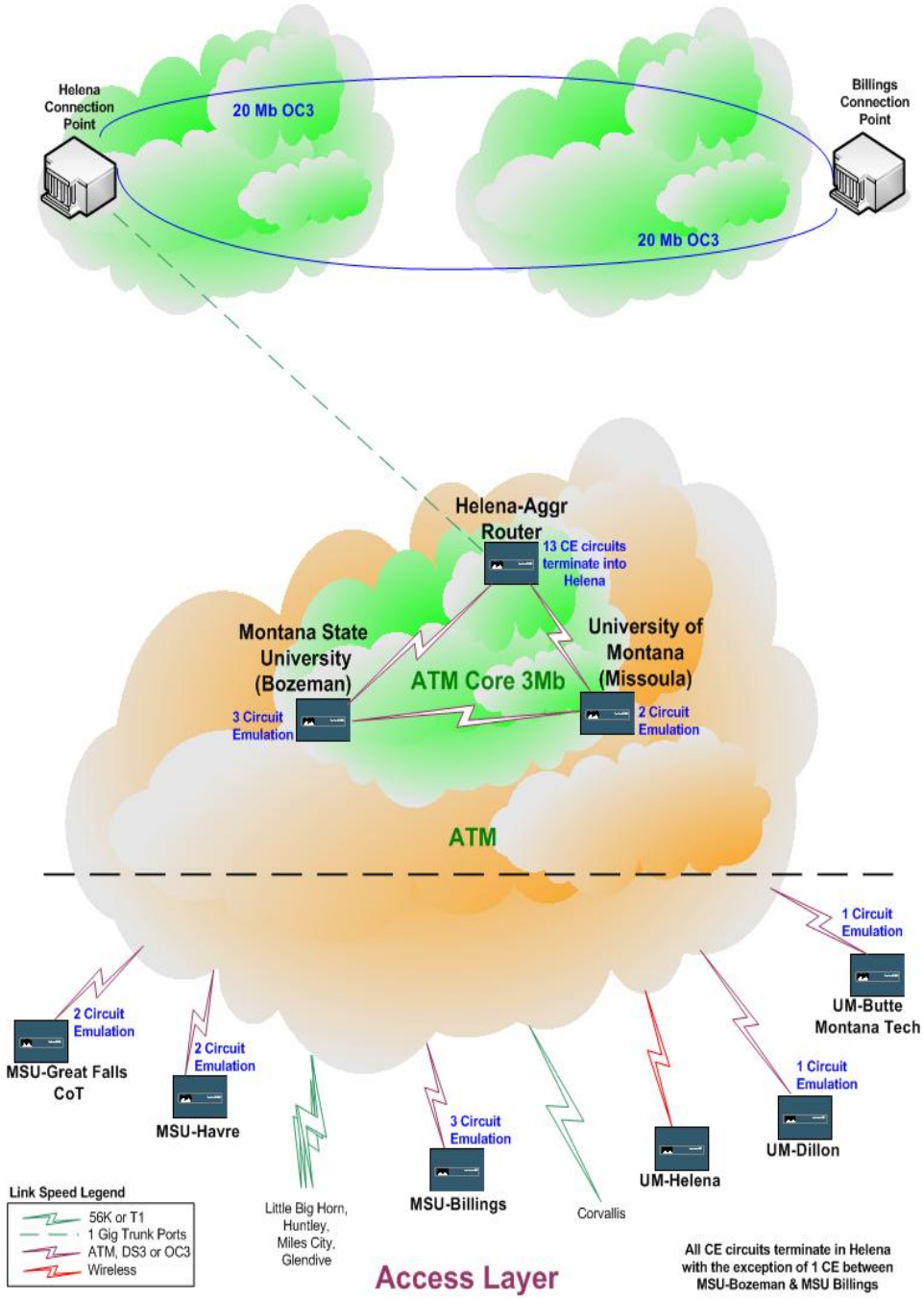

Figure 2.7.2.4a

2.7.3 LOCAL GOVERNMENT (CITY/ COUNTY)

Thirty-four of the fifty-six Counties are currently connected to SummitNet without inspection through a firewall. The issues with this are discussed in Network Transport section 2.7.3.2.

Local government users are typically accessing the Internet and the IBM mainframe. When the local government connection is placed on the DMZ for un-secured access, the mainframe users pass through firewall inspection to gain access.

2.7.3.1 GOALS

The goal is to provide adequate bandwidth and access to State resources to all subscribed local government entities.

2.7.3.2 ISSUES AND CONCERNS

The three issues and concerns for the local government model are:

1. Directly connected to SummitNet
2. State employees connected to the local government networks
3. Pricing for Internet filtering software

1. DIRECTLY CONNECTED TO SUMMITNET

The existing connections that are directly connected to SummitNet bypass all inspection such as firewalls. This poses a security risk. When devices or servers at these counties become compromised, SummitNet is also compromised. The connections need to be relocated to the DMZ for Non-State entity access as described in Network Transport section 2.5.

2. STATE EMPLOYEES CONNECTED TO THE LOCAL GOVERNMENT NETWORKS

In some instances, there are State employees on the local government networks. When the local government networks are placed on the un-secured DMZ, these State workers will need to pass inspection through a firewall to the secured resources of SummitNet.

3. PRICING FOR INTERNET FILTERING SOFTWARE

Today if a local government user accesses the Internet from SummitNet, Surf Control Internet filtering software enforces the State of Montana policy regarding acceptable use. Surf Control is priced by each IP address accessing the Internet. When the number of local government connections increase, the annual cost will also increase.

2.7.3.3 PRINCIPLES

The principle for local government connections is to treat these connections as un-secured and place the connections into a DMZ for inspection through a firewall. If the traffic is destined for the Internet, the traffic never touches SummitNet, but is routed directly to the Internet. If the traffic is destined for SummitNet, the traffic passes inspection prior to admittance.

2.7.3.4 MODEL

The connection model for un-secured access is described in Network Transport section 2.5.

2.7.4 K-12 SCHOOLS AND SCHOOL DISTRICTS

Individual schools and school districts are generally connecting to SummitNet to gain access to the Internet. These connections are generally dedicated and un-secured.

This type of connection requires software that limits the types of Internet web access allowed.

In the future it is possible these entities will use resources from the Office of Public Instruction (OPI) in addition to Internet access.

2.7.4.1 GOALS

The overall goal of K-12 schools and school district connections is to provide a convenient way to access the Internet that is secure and protects school children from accessing inappropriate sites.

Additionally, the educational entity must be able to securely attach to services offered by OPI.

2.7.4.2 ISSUES AND CONCERNS

The primary issue and concern is the inability to calculate the bandwidth needs of the schools and school districts.

2.7.4.3 PRINCIPLES

The primary principle is to provide a reliable and scalable method of accessing SummitNet and its resources.

2.7.4.4 MODEL

The connection model for un-secured access using dedicated circuits is described in Network Transport section 2.5.

2.7.5 VENDORS/ CONTRACTORS

There are many vendors and contractors who do business with the State on a daily basis. It is in the State's interest to continue to have data connections to these entities for electronic data exchange. Vendor and contractor connections are done at the discretion and cost of the requesting agency to support their business requirements. These connections today all terminate outside the DMZ and are inspected twice (through two sets of firewalls).

2.7.5.1 GOALS

The overall goal of vendor/contractor connections is to provide a convenient way to access the resources within SummitNet while protecting the integrity of SummitNet.

2.7.5.2 ISSUES AND CONCERNS

At this time, vendor and contractor connections have no outstanding issues or concerns.

2.7.5.3 PRINCIPLES

The primary principle is to provide a reliable and scalable method of accessing SummitNet and its resources.

2.7.5.4 MODEL

If the vendor or contractor does not require a dedicated connection, Virtual Private Network (VPN) is the accepted method for access. The VPN concentrator is located in the Mitchell building. The connection model for un-secured dedicated circuits is described in Network Transport section 2.5.

2.7.6 REMOTE ACCESS

There are two types of remote users of SummitNet; non-State and State secured. If the user is non-State refer to Network Transport section 2.7.5 Vendors/ Contractors.

2.7.6.1 GOALS

The goal is to provide secure yet flexible method for remote access to SummitNet resources.

2.7.6.2 ISSUES AND CONCERNS

Users and devices accessing SummitNet by a Local Area Network (LAN) or Metropolitan Area Network (MAN) are managed by ITSD. Remote access to SummitNet is not managed by ITSD. Any agency is able to install a Citrix gateway and begin allowing users to access SummitNet. This is a security risk for SummitNet. Since the remote user does not require an account in the Enterprise AD, the user is not authenticated nor accounted for.

2.7.6.3 PRINCIPLES

Remote access must be managed as if the connections were a LAN or MAN.

2.7.6.4 MODEL

The model for remote access is the use of VPN or Enterprise Citrix gateways.

3.0 NETWORK SERVICES

The network services within this document are defined as services integral to the running and delivering of user applications and services within SummitNet. This section discusses the five fundamental services and how they are deployed. The services are:

1. Internet Protocol (IP) Routing
2. Multicast Routing
3. Domain Name Services (DNS) and Dynamic Host Configuration Protocol (DHCP)
4. Wireless Technologies
5. Unified Messaging

3.1 INTERNET PROTOCOL (IP) ROUTING

Since SummitNet has thousands of computers linked together, there must be some agreed-upon way for the devices to address one another and communicate. It is not feasible for each computer to keep track of the individual address of every other computer on SummitNet due to the large volume of individual addresses that would need to be sent to each computer on the network. This would require large amounts of bandwidth, and large computers to store the addresses. To accomplish this task, single vendor routers are installed within SummitNet. These routers direct traffic through SummitNet, based on information learned from network protocols.

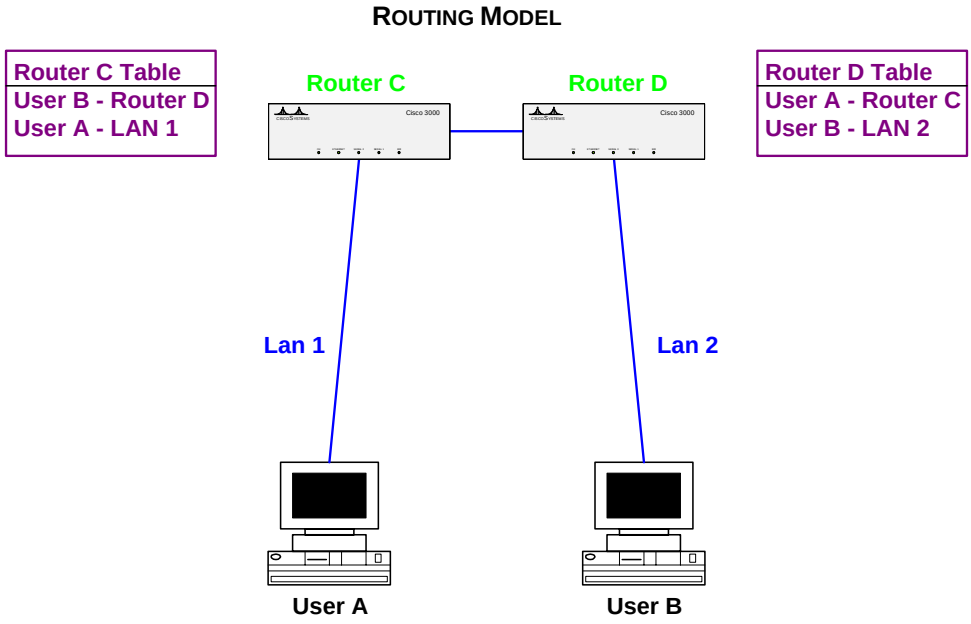

Figure 3.1a

The routing model in Figure 3.1a shows the routing tables for router C and router D. The computer represents all computers in SummitNet and has no routing tables. When User A needs to communicate with User B, User A will send the data onto LAN 1, which is received by Router C. Router C looks up the routing information for User B in its routing table and sends the data onto Router D. Router D looks up the routing information for User B in its routing table and sends the data onto LAN 2, which is then received by User B.

IP is the supported protocol of SummitNet. SummitNet is divided into several hundred individual IP networks. These networks need to be able to communicate with each other and share data. Routers handle the communication between networks. The routers need to know how to get to the networks. Routers do this by either having the routes manually entered for the networks and how to get to them, or implementing a routing protocol that automatically distributes the routing information. SummitNet uses routing protocols. There are two types of routing mechanisms within the network, Interior Gateway Protocol (IGP) and Exterior Gateway Protocol (EGP). IGP is used within SummitNet, where as EGP is used on the networks facing the Internet.

3.1.1 GOALS

The overall goal of the IP routing design is to provide a user traversing SummitNet the most efficient and fastest path to the network services while consuming the least amount of bandwidth for routing updates. To achieve this goal the following must be met:

- Provide the most efficient and fastest path for traffic to traverse SummitNet
- Detect and isolate routing loops
- Efficiently support the use of address space (variable size sub-nets)
- Minimize router memory needs
- Minimize route calculation times avoiding problems with transient loops and unreachable routes
- Minimize congestion
- Minimize route flapping
- Discover new routers, links, and paths automatically

The goal of IP routing is to deliver routing information securely and reliably using as little bandwidth as possible. The solution must be able to provide redundancy, and be easy to install and manage.

3.1.2 ISSUES AND CONCERNS

IGP

The IGP used within SummitNet has been in place for several years and is a well thought out, well-implemented strategy.

The one exception is the ability for any router within the network to participate in the generation and propagation of routes. Routers are not authenticated before being allowed to join the routing domain. The possibility of a rogue router being added to the network with the ability to alter our routing information exists.

EGP

The State does not have an implementation of an EGP. The State relies on the ISP (Visionnet) to announce and propagate the State's public IP address space to the Internet.

3.1.3 PRINCIPLES

To achieve the principle of finding the most efficient and fastest path to any user or service within SummitNet the following objectives must be met:

1. Use of standards-based IGP and EGP
2. Small routed networks
3. Distributing sub-sets of the routing tables
4. Use of Hot Standby Router Protocol (HSRP) for IGP

1. USE OF STANDARDS-BASED IGP AND EGP

The IGP of choice for the State is Enhanced Interior Gateway Routing Protocol (EIGRP). EIGRP is a proprietary protocol and can only be used with Cisco equipment. While EIGRP is designed for small networks and does not scale well, it is extremely easy to configure, manage, and troubleshoot. This makes it an excellent choice for the State. The key advantage that EIGRP has over all other routing protocols is its efficient use of bandwidth. EIGRP does not send out entire routing tables when it sends out routing updates. When the state of a link or router changes, EIGRP sends out only the information necessary to those needing to hear about it, instead of sending the entire routing tables to all neighbors. This design feature alone can reduce the routing traffic on the network by 40% to 50%.

When routing information needs to be exchanged with a non-Cisco device such as an IBM mainframe, Open Shortest Path First (OSPF) routing protocol is used.

To achieve the principle of minimal bandwidth use for routing updates, Route Summarization will be used. EIGRP minimizes the use of bandwidth with the optional use of route summarization.

The State relies on its Internet provider Visionnet to handle all advertising of its assigned public network address space of 161.7.0.0/16. This method of route advertisement is a practical and simple solution for handling routes. Moving forward, the State intends to implement redundancy and diversity for the DMZ between Billings and Helena as well as install an alternate ISP for emergencies. When this happens it becomes necessary for the State to manage and advertise its own address space. This is best done with Border Gateway Protocol (BGP).

BGP is an inter-autonomous system routing protocol. An autonomous system is a network or group of networks under common administration and with common routing policies. BGP is used to exchange routing information for the Internet and is the protocol used between ISPs.

There are two flavors of BGP, eBGP and iBGP. eBGP or Exterior Border Gateway Protocol is BGP when used with a registered Autonomous System (AS). The AS number identifies the owner and the user is then allowed to advertise address space directly to the Internet. eBGP is to be used on our external facing routers to the Internet. iBGP or Interior Border Gateway Protocol is BGP when used internally within a network in conjunction with an internal non-advertised AS. The State intends to use iBGP below the Internet facing routers to manage the DMZ address space and determine which Internet facing router advertises which address space.

2. Small routed networks

Networks should be based on geographical areas, such as a floor in a building, or a remote office. Networks can also be based on work groups, such as Department of Administration or Department of Revenue. These networks ideally contain less than 100 devices. By keeping the size of the network small, the amount of broadcast packets (packets which every machine receives) is reduced. Troubleshooting a smaller network is much easier than troubleshooting a large network. Networks should never span buildings or locations unless there is a sound technical reason for doing so.

3. Distributing sub-sets of the routing tables

Not all routers need to know about every route within the network. Some routers such as remote offices, which have a single connection into SummitNet, only need to know about the route of the next upstream router. Since one route is sent to the remote office instead of the whole routing table, bandwidth usage is reduced.

4. USE OF HOT STANDBY ROUTER PROTOCOL (HSRP) FOR IGP

Each computer on a network must be configured for a default gateway. This is usually done via Dynamic Host Configuration Protocol (DHCP). The default gateway is where all network traffic destined for networks other than the computers own network are sent. EIGRP has the feature for Hot Standby Router Protocol (HSRP). This allows more than a single router the ability to announce a default gateway for any given network. In the event the primary router fails, the standby router or routers take over the function of the default gateway.

3.1.4 MODEL

Each and every router within SummitNet uses EIGRP for its IGP, with the exception of routers not connecting to Cisco equipment such as an IBM Mainframe. Even the smallest remote office is running an instance of EIGRP. All remote offices connect to a POP router in either Helena or Billings. These aggregation routers in turn are connected back to the Helena Capitol complex routers in the Mitchell building. The Capitol complex core routers and the aggregation routers contain full routing tables. Additionally the Capitol complex core routers are configured to run HSRP for all networks contained in the Capitol complex.

Static routing is only used on an exception basis in instances where, for security reasons routing tables should not be distributed.

Figure 3.1.4a illustrates the Capitol complex and the IGP routing model.

IGP ROUTING MODEL

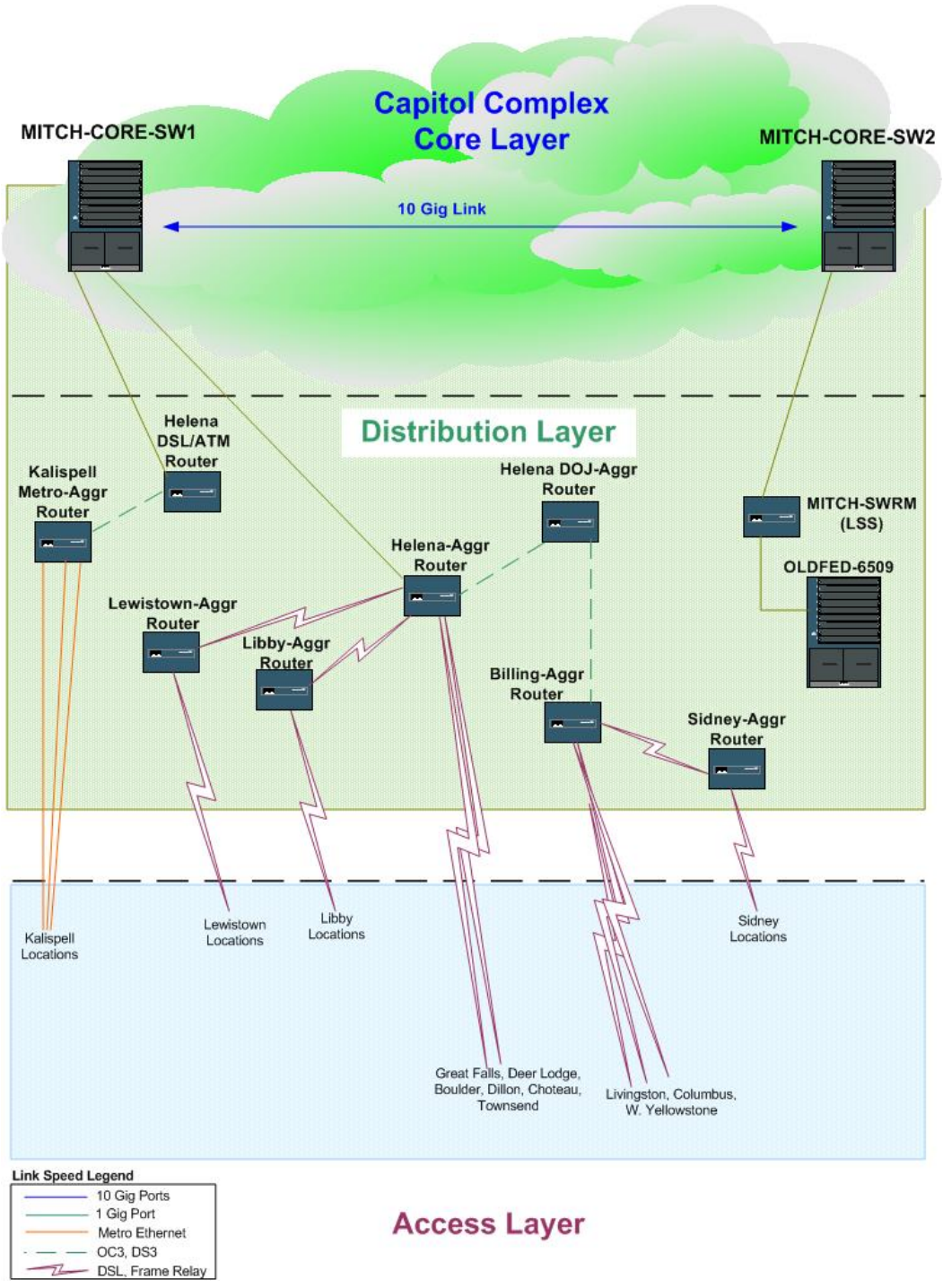

Figure 3.1.4a

Figure 3.1.4b illustrates the EGP routing model using eBGP and iBGP within the DMZ and Internet networks. The blue shaded area represents the eBGP routing area, and the grey shaded space represents the iBGP routing area.

EGP ROUTING MODEL

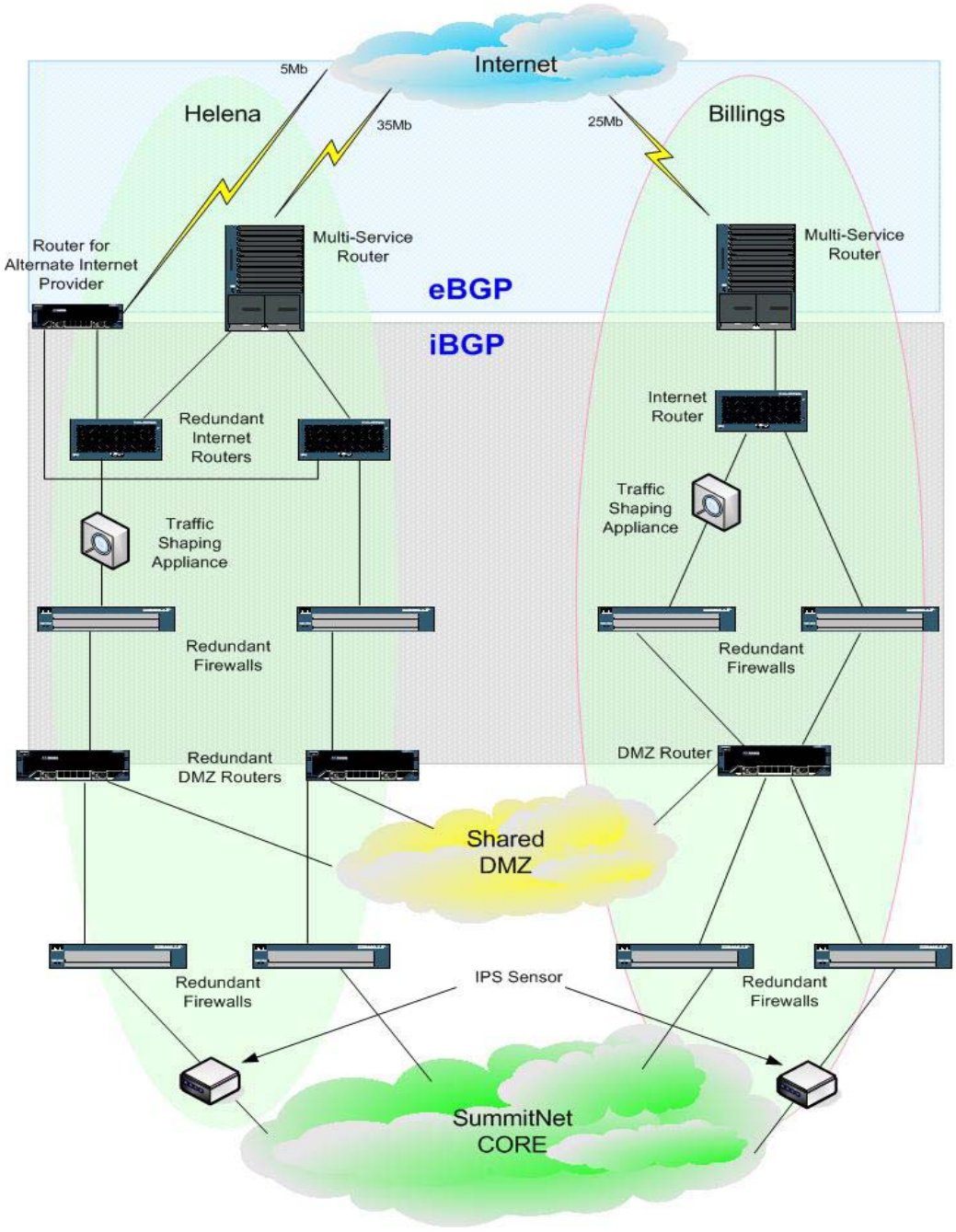

Figure 3.1.4b

3.2 MULTICAST ROUTING

Multicast is a method of delivering a single packet to many clients. It is often referred to as point to multipoint. Multicast conserves bandwidth by simultaneously delivering a single stream of information to many clients. Applications that take advantage of multicast include video conferencing, distance learning, voice systems, stock quotes and news.

IP Multicast delivers source traffic to multiple receivers without adding any additional burden on the source or receivers while using the least network bandwidth of any competing technology. Multicast packets are replicated in the network by Cisco routers enabled with Protocol Independent Multicast (PIM) and other supporting multicast protocols resulting in the most efficient delivery of data to multiple receivers possible.

3.2.1 GOALS

The goal of multicast is to reduce the overall bandwidth consumption.

3.2.2 ISSUES AND CONCERNS

Multicast is designed around the concept of groups. Each client registers with the group that it wants to receive data from. The group does not have any physical or geographical boundaries; the hosts can be located anywhere within SummitNet. The process of generating the multicast groups and the registration of the clients to the individual groups can become quite cumbersome if not installed and managed properly.

3.2.3 PRINCIPLES

Multicast must be easy to implement and manage. It should also scale easily for new multicast services.

To achieve ease of implementation, scalability, and manageability, multicast has been divided into two areas:

1. The Client
2. The Service

CLIENT:

There are two methods in use for registering the clients. One is the industry standard of Internet Group Management Protocol (IGMP). The second method is the use of Cisco proprietary Cisco Group Management Protocol (CGMP).

IGMP has been chosen due to its ease of implementation. When a switch supports IGMP, no configuration of the router is required to begin registering clients. If a switch does not support IGMP, then CGMP is used. To use CGMP, it must be configured on the router interface.

SERVICE:

Each multicast service must be manually configured on the router. This is done by assigning each multicast service a Rendezvous Point (RP) on the router. The RP points the client to the identity of the service. The RP can either be statically assigned or automatically known. For ease of use and manageability, the auto-RP function has been chosen as the method to define RPs. Auto-RP allows for automatic registration of the RP.

In the event of a router failure, the RP should automatically failover to the secondary router. Cisco's automatic failover for RP is Anycast RP. Anycast RP is an implementation strategy that provides load sharing and redundancy in PIM sparse mode networks. Anycast RP allows two or more rendezvous points (RP) to share the load for source registration and the ability to act as hot backup routers for each other.

To keep the router from flooding the network with multicast packets looking for a service address (RP), each interface containing clients and or the service is configured with PIM. There are two forms of PIM:

1. Dense mode
2. Sparse mode

When a multicast source begins to transmit data, PIM forwards the data to all its PIM neighbors. Those PIM neighbors then forward the data to their PIM neighbors. This happens throughout the network whether there are group members on the router or not. This can result in the network being flooded with multicast traffic. This is traditional or dense mode PIM. Cisco has a modified version of PIM called sparse mode PIM. PIM sparse mode relies on the RP to understand the path of the multicast traffic and does not flood the network with multicast. PIM sparse mode is the preferred multicast method.

3.2.4 MODEL

As shown in Figure 3.2.4a, the routers are configured for Auto-RP and Anycast RP. The interfaces containing multicast source or destination are configured for PIM Sparse mode. Since the majority of the switches in our network support IGMP, there is no configuration required for the multicast client.

Figure 3.2.4a illustrates the devices configured allowing Multicast to be delivered within the LAN.

Figure 3.2.4a shows the network interface with the multicast source configured for PIM Sparse mode. The two Helena campus core 6509 switches with route processor modules are configured with Auto Rendezvous Point (RP) and Anycast Rendezvous Point (RP). The switches downstream from the 6509 core switches are all configured for PIM Sparse mode. Finally the access layer switch containing the client is configured for IGMP.

PROPOSED MULTICAST MODEL

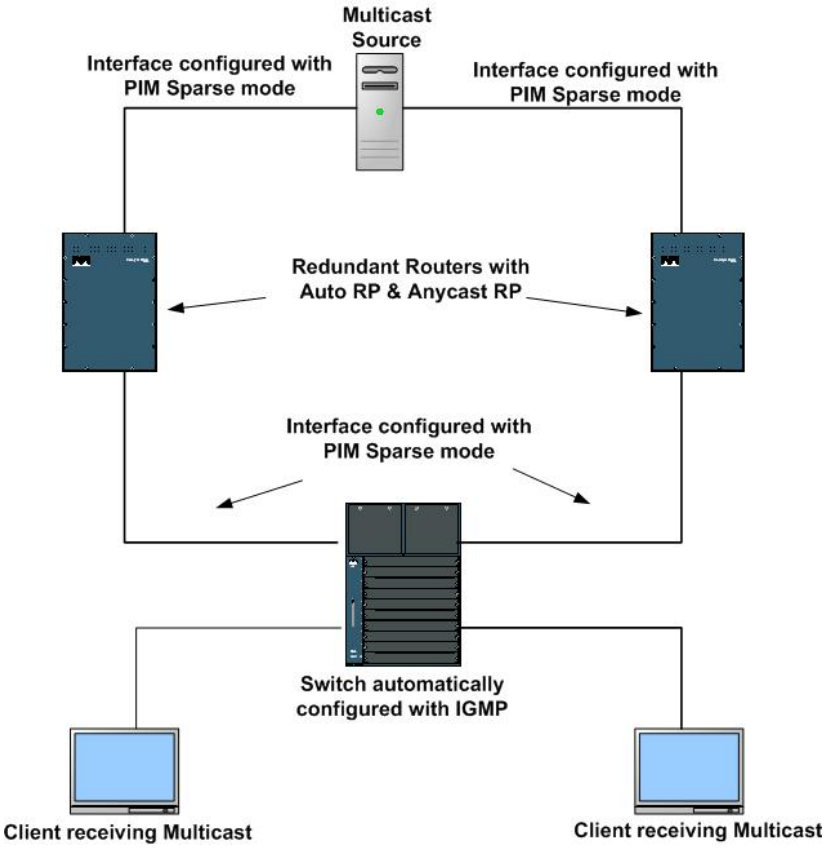

Figure 3.2.4a

3.3 DOMAIN NAME SERVICE (DNS) AND DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

This section describes the use of the Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP) within SummitNet. It gives a brief overview of the system, specifically reviewing those parts of the DNS and DHCP systems that are of special interest in the State environment. DNS is used extensively within SummitNet and the Internet.

Domain Name Service is a service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet and SummitNet are based on IP addresses. Every time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4

The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

The purpose of the DNS is to translate back and forth between names that people can understand, like WWW.MT.GOV and Internet protocol addresses that computers and routers can understand, like 146.146.55.10. Theoretically, a simple table of names and numbers would suffice, but administering this table would require universal knowledge and complete control and authority. By 1984, the Internet had grown so large that no single person could have control, or even knowledge, of the entire network.

An agency host in an agency may be known by up to three different addresses. The response to a DNS query about a particular host depends on who asks. Another host in the same agency should receive the local address; a host out on the Internet should receive the public address or none at all.

Dynamic Host Configuration Protocol is an Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses, to deliver TCP/IP stack configuration parameters such as the subnet mask and default router, and to provide other configuration information such as the addresses for printer, time and news servers.

Dynamic Host Configuration Protocol is used when computers are added to a network, because the IP address and TCP/IP settings are necessary for the host to participate in the network. These DHCP settings are periodically refreshed (it expires, meaning the client must obtain another assignment) with typical intervals ranging from one hour to several months, or can be set to never expire.

The DHCP server ensures that all IP addresses are unique, that is, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). The IP address pool management is done by the server and not by a human network administrator.

3.3.1 GOALS

The goal is to offer an enterprise class Domain Name Service (DNS) to manage and deploy IP addresses. The DNS architecture must be scalable, secure and easily managed. DNS's primary goal is to correlate domain names to IP addresses. On the SummitNet network, DNS assigns an authoritative domain name without using an external central registrar for each inquiry. DNS must be scaled to handle denial of service attacks, and provide an authoritative name service for all Internet facing domains.

The DNS system must be able to load balance domain names. For example if the Secretary of State offers services in both Helena and Billings, there must be an automatic method of load balancing the connections to the servers.

3.3.2 ISSUES AND CONCERNS

Issues and concerns that need to be addressed include the extent of using dynamic DNS to integrate DHCP with the enterprise directory architecture (Microsoft's Active Directory).

Today Microsoft handles DNS. The DHCP system used today is MetaIP. While this system is delivering DHCP for the State, it is not considered an enterprise solution by industry standards.

3.3.3 PRINCIPLES

Domain Name Service is a hierarchical, distributed database. Its design reflects the fact that no one organization controls, or even knows about, names and addresses throughout the Internet, but that each organization has authority over some part of it. The Internet Network Information Center, or InterNIC, has authority for the root of the hierarchy, called the *root domain*, or sometimes *dot*. (This domain is often written *"."*.) It also has authority for the top-level domains EDU, COM, GOV, NET, ORG, and so on. The InterNIC has delegated authority over the next level down, as well as the country domains, like UK, CN, HK, TW, US, AU, to other organizations. For example, it has delegated authority for the domain APPLE.COM to Apple Corp.

With authority comes responsibility. Apple Corp. has the responsibility to set up DNS for all of APPLE.COM. Apple Corp. may decide to further divide this domain into SUPPORT.APPLE.COM, SOFTWARE.APPLE.COM, INFO.APPLE.COM, and many others. Furthermore, Apple Corp. may delegate authority for INFO.APPLE.COM to someone else. Thus Apple Corp. has authority for three domains: APPLE.COM, SUPPORT.APPLE.COM, and SOFTWARE.APPLE.COM.

DNS and DHCP should be able to do the following:

- Conserve available addresses and eliminate manual configuration and management of IP addressing
- Have the ability to multi-home to multiple ISPs
- Make efficient use of IP address space
- Feature ease of administration
- Allow for automatic failover
- Allow for load balancing of domain names

3.3.4 MODEL

While the systems delivering DNS and DHCP for the State are adequate, an annual review of this process and emerging enterprise solutions is recommended.

Figure 3.3.4a illustrates normal DNS function currently in use. 1.) The user makes an initial request to www.mt.gov. 2.) The request is forwarded to the DNS server. 3.) If the DNS server has an entry for www.mt.gov it responds back to the user with the IP address of the server. 4.) The user then connects directly to the mt.gov server.

NORMAL DNS INFORMATION FLOW

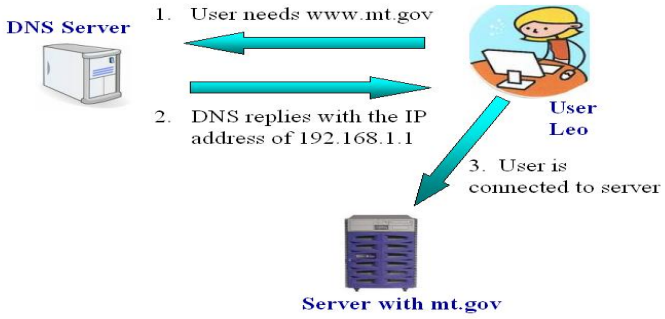

Figure 3.3.4a

There are times when several servers can respond to a domain name. It is also possible the servers do not reside in the same physical location. In these cases it is necessary to load balance the domain name requests. The Global Site Selector (GSS) by Cisco load balances domain name requests between locations. The GSS is comprised of a primary and standby. The primary GSS is located in Helena, and the standby GSS is located in the Billings Services Center. The example in Figure 3.3.4b shows DNS using the GSS to load balance domain name requests between locations.

Figure 3.3.4b shows 1.) The user makes an initial request to www.mt.gov. 2.) The request is forwarded to the DNS server. 3.) The DNS server queries the GSS. 4.) The GSS load balances the two locations and sends the user back the information for the Billings server. 5.) The user then connects to the server with www.mt.gov.

NORMAL DNS WITH GSS INFORMATION FLOW

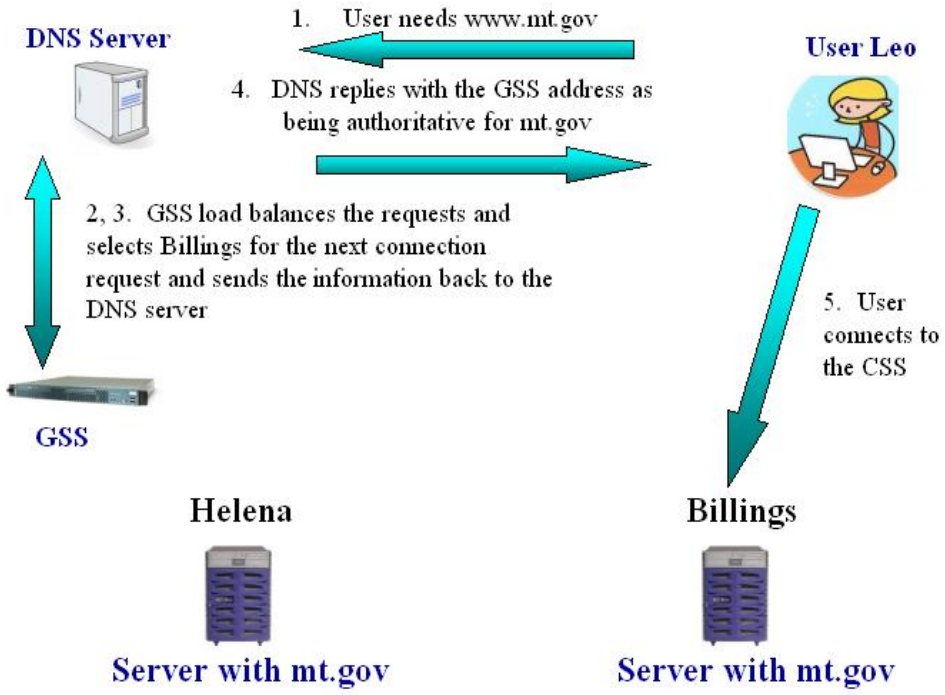

Figure 3.3.4b

It is possible a location may have more than one server answering for the domain. When more than one server exists in a location, the servers must be load balanced. This is accomplished with the Content Services Module (CSM) in Helena, and the Content Services Switch (CSS) in Billings.

The CSM is a blade located in the core 6509 switches. The primary CSM is located in switch 1, and the redundant CSM is located in switch 2.

Figure 3.3.4c illustrates normal DNS function with site and location load balancing.

Figure 3.3.4c shows 1.) The user makes an initial request to www.mt.gov. 2.) The request is forwarded to the DNS server. 3.) The DNS server queries the GSS. 4.) The GSS load balances the two locations and sends the user back the information for the Billings server. 5.) The user asks for a request to www.mt.gov via the CSS. 6.) The CSS forwards the connection request to the selected server.

NORMAL DNS WITH GSS, CSS, AND CSM INFORMATION FLOW

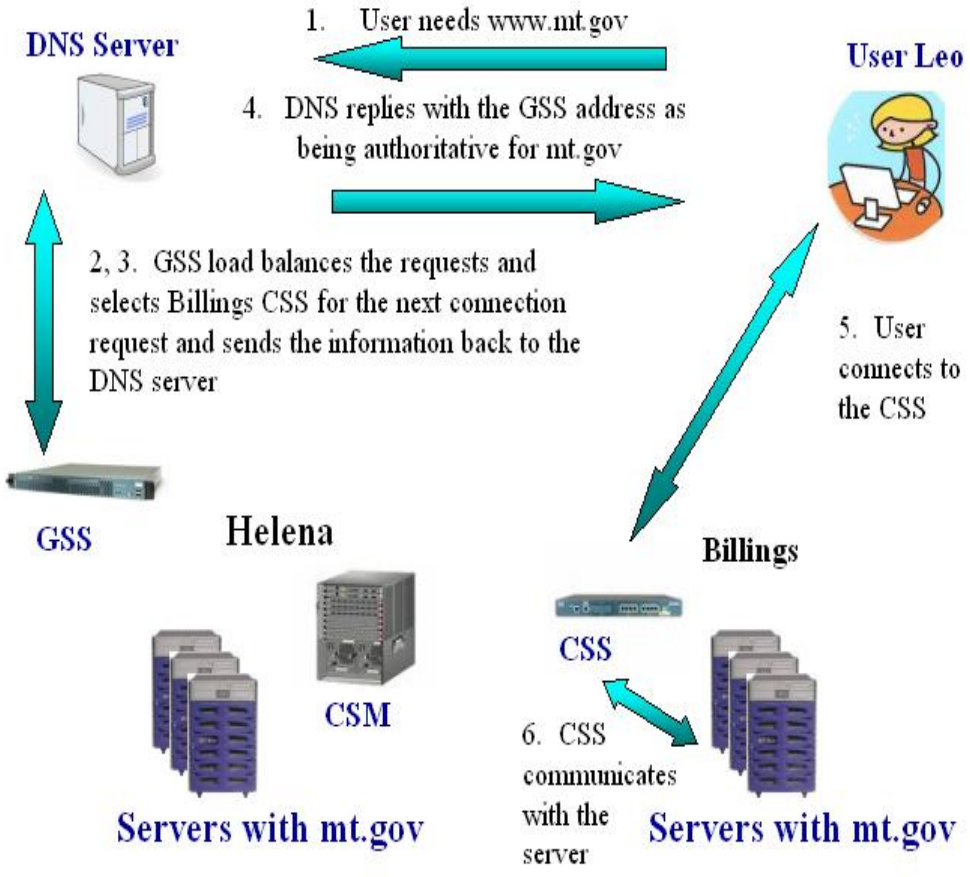

Figure 3.3.4c

Normal DHCP function is illustrated in Figure 3.3.4d.

Figure 3.3.4d shows 1.) The user turns on the PC and the PC automatically requests an IP address. 2.) The enterprise DHCP server replies with the IP address, WINS server, DNS server information, default gateway, STATE.MT.US domain name, and a 6 day lease.

NORMAL DHCP MODEL

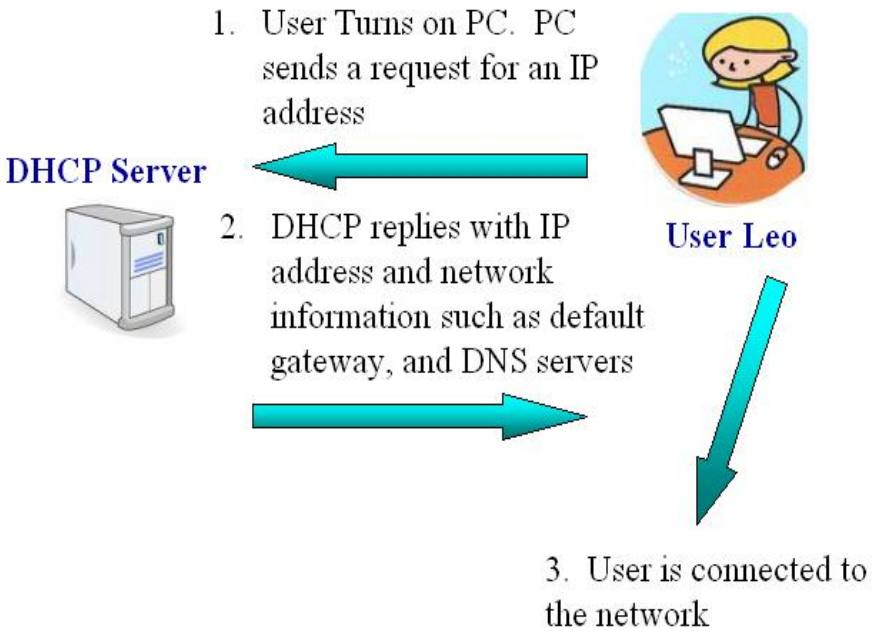

Figure 3.3.4d

3.4 WIRELESS TECHNOLOGIES

The State of Montana is currently deploying a wireless LAN system. This system is divided into two types of access:

1. Guest access for non-secured users
2. Secured access for State users

This system is available in most public areas within the Capitol Complex.

3.4.1 GOALS

The goal of the wireless system is to deliver non-secured (Internet only) and secured (trusted into SummitNet) network access.

The wireless solution must eliminate unauthorized access to wireless networks, unauthorized capture of wireless traffic and unauthorized placement of rogue access points. It must also offer roaming, self-healing coverage, simple network management, achievable service levels, and quality of service.

3.4.2 ISSUES AND CONCERNS

The wireless Access Points (APs) currently being deployed are autonomous in nature, each containing a configuration similar to a router. This type of deployment and management is time consuming. The newer wireless systems are controlled by a centralized management system or controller system. The controller-based system allows for a central configuration file that is automatically pushed out to a new AP.

A major issue with wireless systems is the limited numbers of radio channels available and the need to keep adjacent APs operating on different channels to prevent cross channel interference. Next generation controller based systems automatically make channel assignments and set AP transmitter power levels to optimize RF coverage while Minimizing interference. In the event of an AP failure, adjacent APs are automatically adjusted to fill in the coverage gap left by the failed AP.

3.4.3 PRINCIPLES

There are two types of wireless users:

1. Non-Secured users
2. Secured users

The non-secured user is neither authenticated or authorized and is not permitted any access to resources within SummitNet. The non-secure user is ported directly to the Internet upon completing registration.

All secured wireless access uses 802.1X authentication. The devices are authenticated using Cisco Access Control Server (ACS) and the enterprise Active Directory (AD). The Access Control Server is used to authenticate, authorize and account (AAA) devices and users. This device uses the IETF standard of RADIUS. The ACS authenticates the device and user by accessing the Enterprise Active Directory (AD). If the user or device is not validated, admittance to SummitNet is denied. Non-State devices are not allowed onto the secured wireless network.

The secure wireless system uses WPA2 with AES and integrity check (MIC) for encryption.

Extensible Authentication Protocol (EAP_PEAP) is the method of authentication used in conjunction with 802.1X for the secured wireless user.

3.4.4 MODEL

NON-SECURED WIRELESS

Non-secured users register themselves and accept the State of Montana's Internet Acceptable Use Policy. The user is then granted access to a separate isolated, virtual network (VLAN) that is passed directly to the firewall and out to the Internet.

The non-secured client may use any supplicant and wireless card, configured for no authentication or encryption. The user connects to the broadcasted SSID of guest. Once the wireless connection is established, the user opens up Internet Explorer and is redirected to the registration page. At this time the user provides contact information, and accepts the State of Montana's Internet Acceptable Use Policy.

The entire process is managed by Cisco's Broad Band Services Manager (BBSM) product.

To control the amount of bandwidth non-secured users can consume to the Internet, the bandwidth is managed and is not allowed to exceed a combined throughput of 3Mb. The data is not traffic shaped nor does it have QoS policies applied. The traffic is first in first out (FIFO).

Figure 3.4.4.a illustrates the non-secured user and network admittance.

Figure 3.4.4a shows 1.) Client connects to the isolated wireless network and is not able to communicate with anything except the AP and BBSM. The BBSM leases the client a DHCP address. 2.) Once the user attempts to connect to the Internet, the BBSM sends the client a login web page and the Internet Acceptable Use policy. The client is still restricted to communicating only with the AP and the BBSM. 3.) Once the user agrees to the Internet Acceptable Use policy, the client is allowed to access the Internet. The user remains on the isolated wireless network.

NON-SECURED (GUEST) WIRELESS ACCESS MODEL

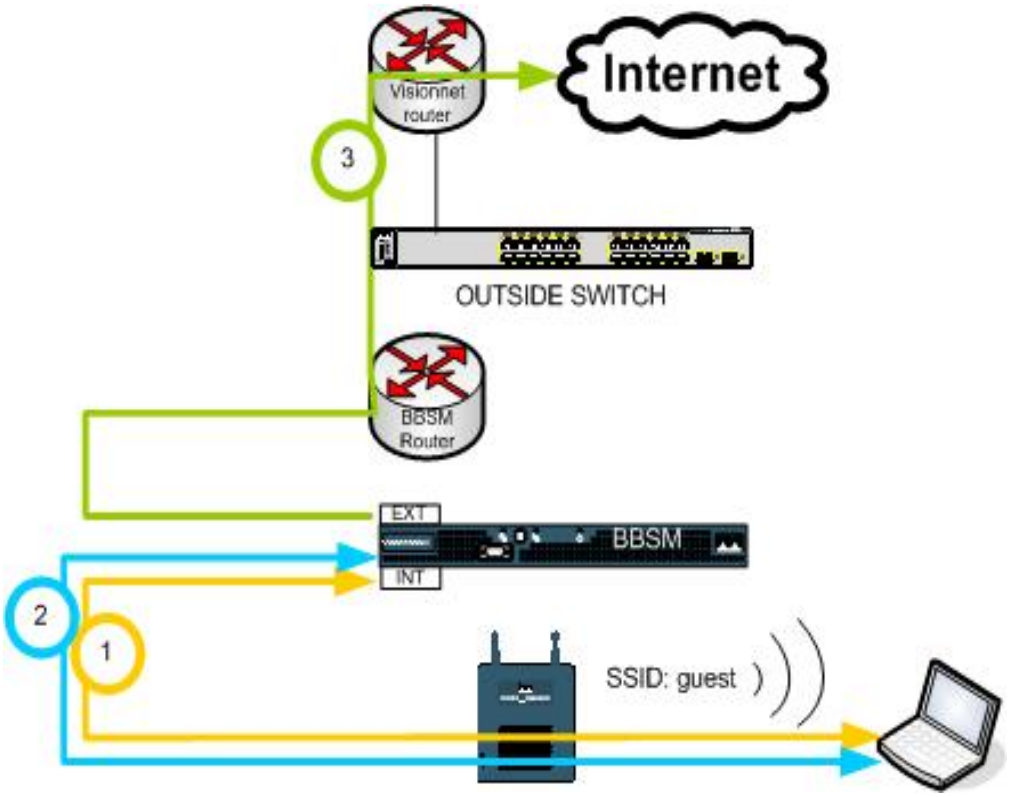

Figure 3.4.4a

SECURED WIRELESS

The SSID for secure access is not broadcast. At this time only the Cisco wireless client adapter coupled with Juniper's Odyssey client are supported for secured wireless access. The client must contain the trusted certificate for the ACS, be configured for WPA2 with AES, CCM, and EAP_PEAP.

As previously stated, the entire authentication and authorization process is managed by the ACS and the Enterprise AD. All wireless APs needing to authenticate and authorize users forward the requests on to the closest Wireless Domain Services (WDS). The WDS then forwards the request onto ACS. Non-State machines are not allowed onto the secured wireless network. The machine or device must exist in the enterprise Active Directory.

Once the wireless user is admitted to SummitNet, the user has access to all SummitNet resources. The secured wireless user has all the same rights and privileges as a wired user. Internet bound traffic is not restricted with bandwidth constraints. The traffic can be policy shaped if necessary, using QoS.

Figure 3.4.4b illustrates the process for authenticating a device and user for secured wireless access.

Figure 3.4.4b shows 1.) Client sends user and machine authentication request to the Wireless AP. (Note: a client can also connect to the Wireless AP WDS). 2.) The AP sends the authentication data encrypted to the primary WDS AP, otherwise to the secondary WDS AP. 3.) The WDS AP verifies client authentication by sending a request to the primary ACS or backup ACS via Radius protocol. 4.) The ACS passes or denies client authentication based on the Enterprise AD and returns attempt results to the WDS AP. 5.) The WDS AP sends the pass or deny attempt results to the client AP. The client is allowed or denied secure access. 6.) If the client is allowed a secure wireless connection, a client record is maintained on the AP and forwarded to the wireless management platform Wireless LAN Solution Engine (WLSE).

SECURED WIRELESS ACCESS MODEL

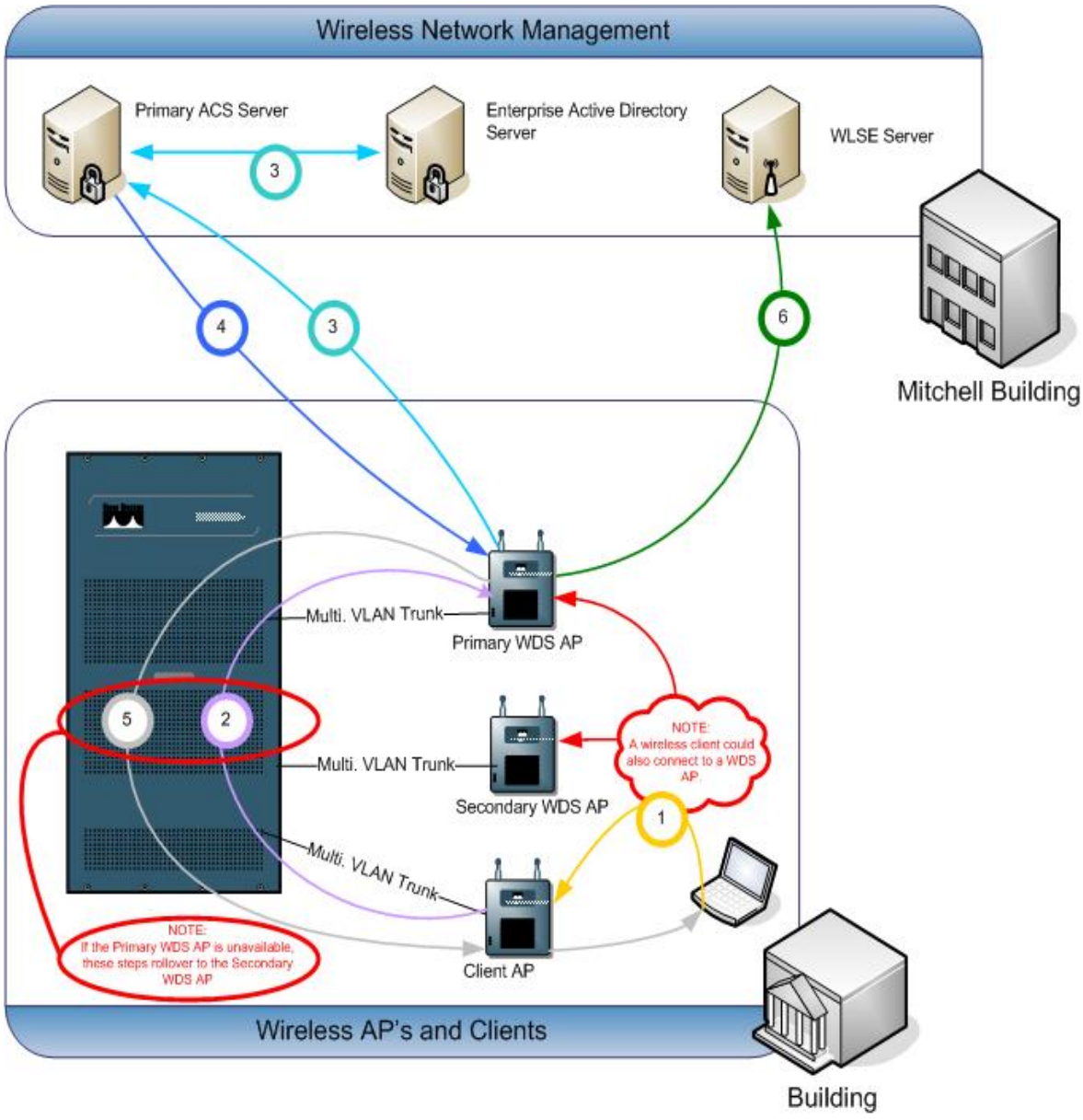

Figure 3.4.4b

For additional information regarding the wireless system and how it is deployed within the State of Montana, refer to the ITSD published document "Wireless LAN Architecture" on the ITSD Agency website www.itsd.mt.gov/policy/itpolicy.asp located in the Network/Telecommunications section.

3.5 UNIFIED MESSAGING

Unified Messaging (UM) is defined as a communications solution that unifies a single message store and directory with a desktop client application, providing users with one central point of access to all their voice, fax, and e-mail messages. Messages are delivered to a single inbox, housed in one central message store, and feature single directory service. This means that users have global addressing capability, and can use a single directory to address all their messages, regardless of media.

Unified messaging solutions are also designed to work with open standards. This means that system administrators have one central point of access for all support and maintenance tasks. Disjointed forms of enterprise communications quickly converge into a unified solution that merges voice, instant messaging (IM), video, collaboration, and presence. This will result in improved organizational efficiency and allow a common platform for communication regardless of the end-user device or application.

3.5.1 GOALS

The goal of Unified Messaging is the integration of different streams of messages into a single source that is accessible from a variety of different devices. These streams include voice, video, email, and fax. This offers simplification because only one infrastructure needs to be managed. This makes it easier for adds, moves and changes.

Unified Messaging is intended to offer, “plug and play” centralized control and has the potential for large cost savings. The aim of deploying UM solutions generally is to enhance workflows and improve processes as well as services. It requires organizational convergence and cooperation between voice, video, and data staff. The deliverables are improved productivity and service delivery. It can be used for distributed call centers and click-to-talk feature sets.

3.5.2 ISSUES AND CONCERNS

Unified Messaging has a large impact on physical infrastructure requirements. It also includes an increased expense for QoS capable network hardware, bandwidth provisioning, predicable latency and cost of providing resiliency.

Unified Messaging involves a basic cultural change in the sense that there is an organizational impact from converged networks. Management expectations must include end-user education, network management, staff training, and the understanding that feature sets may vary. Unified

Messaging also must address concerns with end-to-end encryption, firewall changes, troubleshooting issues, adds/moves/changes, and how to manage client/server voice systems.

Encryption can cause issues with QoS schemes. A solution may possibly involve assigning VLANS and prioritizing the traffic. It should also include greater availability and support of E9-1-1 solutions.

3.5.3 PRINCIPLES

A standards based solution is the best approach. The industry trend has moved away from Voice over Internet Protocol (VoIP) and towards Session Initiation Protocol (SIP). SIP is an application-layer (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include telephone calls, multimedia distribution, and multimedia conferences.

Session Initiated Protocol (SIP) is a better solution than proprietary vendor protocols for handling UM. Session Initiated Protocol enables cross-vendor functionality and has the ability to interface with Exchange and any VoIP system. UM enables enterprises to build a single communications portal that combines voice, e-mail, calendaring, and instant messaging (IM).

Unified Messaging provides a presence that allows users to know where people are located, customization so users can control how they want to be contacted and extensibility so meetings can be tied into conferencing systems such as WebEx. The SIP protocol is used to set up the call, and to tear down the call. The actual call is handled with traditional protocols such as (Real-Time Transport Protocol) RTP.

A motivating goal for SIP is to provide a signaling and call setup protocol for IP-based communications that can support a superset of the call processing functions and features present in the public switched telephone network (PSTN). These features include familiar telephone-like operations: dialing a number, causing a phone to ring, hearing ring back tones or a busy signal.

3.5.4 MODEL

Hardware endpoints - devices with the look, feel and shape of a traditional telephone, but that use SIP and RTP for communication are commercially available from several vendors. Some of these can use Electronic Numbering (ENUM) to translate existing phone numbers to SIP addressing using DNS, so calls to other SIP users can bypass the telephone network. The SIP addressing can be the traditional telephone number or Instant Messaging address, all available via DNS.

The use of a SIP gateway allows for the easy interface of traditional voice systems to function with UM.

The University System currently uses traditional ATM Circuit Emulation (CE) for voice systems around the State. These dedicated circuits are expensive and sit idle if there are no phone conversations. These systems are anticipated to migrate to SIP based solutions in 2007.

Microsoft offers a user-friendly interface for SIP. The user has a contacts database, and SIP knows how to reach the individual user. To access a user via SIP the calling user simply clicks on the icon. Since signaling is part of SIP, if the user is not available via cellular phone, but is available via desk phone, the icon shows the phone available.

Figure 3.5.4a shows a user and their Outlook contacts using SIP.

SIP USER USING OUTLOOK CONTACTS

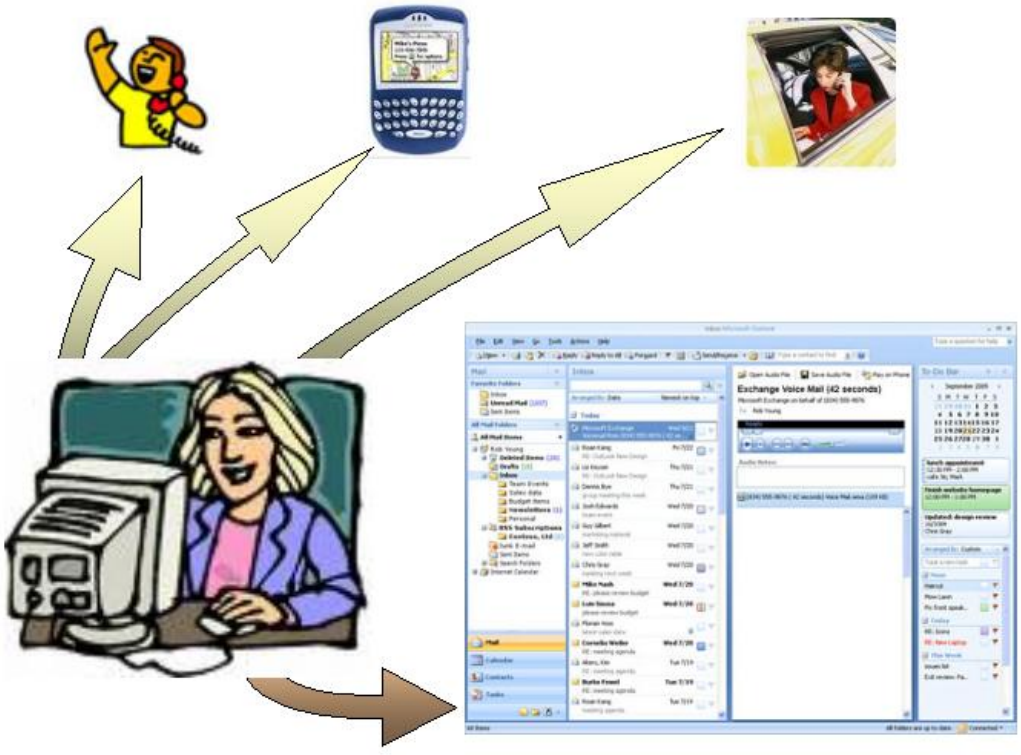

Figure 3.5.4a

4.0 NETWORK SUPPORT

Network Support section to be supplied in a subsequent revision.

5.0 CONCLUSION

As previously stated, modern enterprise telecommunication networks must be scalable and flexible in an increasingly dynamic and complex service environment. As SummitNet evolves from a best effort network to a 7 days a week, 24 hours a day, 365 days a year mission critical entity delivering converged technologies, redundancy, reliability, predictability, and security must be the focus when designing and implementing the State of Montana's next generation network. SummitNet is the foundation on which all agencies and State government rely to get their jobs done. This network strategic plan is crucial in the designing and building of the next generation of SummitNet.

Many of the design models in the Network Transport and Network Services sections are in place within SummitNet or are in the design stage. The models not yet implemented can easily be divided into small projects with staged implementation plans.

Implementation will be handled as individual projects, complete with implementation and project plans.

Network management and operations are addressed in the Network Support section to be supplied in a subsequent revision.

6.0 APPENDIX A

6.0 Glossary of Terms

802.11i - The IEEE standard for Robust Security Network for WLANS (Wireless Local Area Networks). 802.11i includes a strong message integrity check, allows for authentication using 802.1X and uses AES (Advanced Encryption Algorithm) for message encryption. WPA (Wi-Fi Protected Access) is an industry standard based off an early version of 802.11i.

802.11a - 802.11a is an updated, bigger, better, faster version of 802.1b. 802.11a supports speeds up to 54Mbps. 802.11a runs in the 5GHz frequency range, which was allocated by the FCC.

802.11b - 802.11b is the most common wireless local area network. 802.11b is a low power wireless system, so the closer you are to a transmitter, the faster it will be. Wireless operating range (indoors) 100 feet at 11Mbs 165 feet at 5.5Mbs; it operates in the 2.4GHz range.

802.11g - 802.11g allows data rates up to 54Mps in the 2.4GHz range. 802.11g devices work with 802.11b devices.

802.1Q - An IEEE standard for providing VLAN identification and quality of service (QoS) levels. Four bytes are added to an Ethernet frame, increasing the maximum frame size from 1518 to 1522 bytes. Three bits are used to allow eight priority levels (QoS) and 12 bits are used to identify up to 4096 VLANs.

802.1X - 802.1X is an IEEE standard. It provides authentication to devices attached to local area networks, both wired and wireless. 802.1X attempts to introduce serious security checking by making sure that both the user and machine (client device) of the LAN are clean and honest folks who are authorized to use the LAN.

AES - Advanced Encryption Standard. A standard for encryption, which is intended to replace DES (Data Encryption Standard), a standard developed by IBM in 1977 and thought to be virtually un-crackable until 1997. The AES standard specifies a symmetric, or private key algorithm. It is a block cipher supporting key lengths ranging from 128 to 256 bits, and variable-length blocks of data.

ATM - Asynchronous Transfer Mode. A very high-speed transmission technology. ATM is a high bandwidth, low-delay, connection-oriented, packet-like switching and multiplexing technique. Usable capacity is segmented into 53 byte fixed-size cells, consisting of header and information fields, allocated to services on demand.

BGP - Border Gateway Protocol. An inter-autonomous system routing protocol. BGP is used to exchange routing information for the Internet and is the protocol used between ISPs. It is a

Path Vector (PV) type routing protocol. A border router running a path vector routing protocol advertises the destinations it can reach to its neighboring border routers. A path vector protocol pairs each of those destinations with the attributes of the path to it. The attributes include the number of hops (i.e., routers traversed) and the administrative "distance". The attributes of administrative distance weights routes learned from IBGP more heavily than those learned from EBGP. Interior routes are weighted more heavily (and preferred) than are exterior routes, which cross network domains and which, by definition, involve multiple Autonomous Systems.

iBGP - Interior Border Gateway Protocol. BGP running inside an autonomous system (AS) is referred to as IBGP (Interior Border Gateway Protocol). IBGP allows the free exchange of information between trusted systems. A BGP router that routes IBGP traffic is called a transit router. IBGP routes have an administrative distance of 200.

eBGP - Exterior Border Gateway Protocol. BGP running between autonomous systems (AS) is referred to as EBGP (Exterior Border Gateway Protocol). Routers that sit on the boundary of an AS and that use EBGP to exchange information with the ISP are border or edge routers. EBGP has an administrative distance of 20.

CELL - A unit of transmission in ATM and SMDS. A fixed-size packet consisting of a 48-octet payload and 5 octets of control overhead in the form of a header in the case of ATM.

CGMP - Cisco Group Management Protocol. A protocol used exclusively by Cisco, to allow IP hosts and gateways to report their multicast group memberships. When used in concert with a multicast protocol, the IP based network can support multicasting.

DHCP - Dynamic Host Configuration Protocol. DHCP is a TCP/IP protocol that enables PCs and workstations to get temporary or permanent IP addresses (out of a pool) from centrally administered servers.

Data Link Layer - The second layer of the Open Systems Interconnection (OSI) data communications model of the International Standards Organization. It puts messages together and coordinates their flow. A layer that packages raw bits from the physical layer into frames (logical, structured packets for data). This layer is responsible for transferring frames from one computer to another, without errors. After sending a frame, the data-link layer waits for an acknowledgement from the receiving computer.

DMZ - De-Militarized Zone. A partially protected zone on a network not exposed to the full fury of the Internet, but not fully behind the firewall.

DWDM - Dense Wavelength Division Multiplexing is a means of increasing the capacity of fiber-optic data transmission systems by transmitting many wavelengths of light down a single strand of fiber. DWDM supports from 8 to 72 wavelengths. Up to 80Gb X 80 wavelengths is possible with today's DWDM. DWDM has replaced SONET as the broadband optical technique of choice in the carrier industry.

EAP - Extensible Authentication Protocol, as defined in IEFT RFC 2284, is an authentication protocol that runs over Layer 2, the Data Link Layer (DLL), of the OSI Reference Model. As EAP does not require IP (Internet Protocol), it includes its own support message delivery and retransmission. EAP was developed for use over PPP (Point-to-Point Protocol) although it is now in use in IEEE 802 LAN environments, including 802.3 Ethernet LANS, and 802.11 Ethernet WLANS (Wireless LANS).

EGP - Exterior Gateway Protocol. An Internet protocol for exchanging routing information between autonomous systems.

Extended Fiber Channel - A gigabit-speed network technology primarily used for storage networking. Fiber Channel provides a channel connection for dedicated or switched point-to-point connection between devices. Channel connections are hardware-intensive, low in overhead, and high in speed. Fiber Channel supports the transfer of data in frames, with a payload of 2,048 bytes.

ENUM - Electronic Numbering. Maps phone numbers to IP addresses. A proposed standard (RFC 2916) from the IETF (Internet Engineering Task Force) for a DNS-based (Domain Name Server) method for mapping telephone numbers to URLs (Web addresses) and, ultimately, to IP addresses.

Frame Relay - An access standard defined by the ITU-T in the 1.122 recommendations. Employs a form of packet switching analogous to a streamlined version of X.25 networks. The packets are in the form of variable length frames, with the payload of anywhere between 0 and 4.0-96 octets. Frame relay is completely protocol independent.

Gigabit Ethernet - Uses the same framing as Ethernet and Fast Ethernet, but has a much higher clock speed (one billion bits per second).

GIGAPOP – A POP (Point of Presense) with a throughput in the range of a billion (giga) packets per second. GIGAPOPs are being implemented in support of Internet2, a high-speed Internet supported by the National Science Foundation and a project of the University Corporation for Advanced Internet Development (UCAID).

KPI - Key Performance Indicator. Financial and non-financial metrics used to quantify objectives to reflect strategic performance of an organization. They help an organization to measure progress towards their goals, especially toward difficult to quantify knowledge-based activities.

IDS - Intrusion Detection System. A technology that gathers and analyzes information across gateways, servers, desktops to identify possible security breaches that can occur from within or outside an organization. An IDS can detect attacks on the network through the use of statistical analysis of network traffic as well as by monitoring reports and log files to detect abnormal network activity. No action is taken on the packets.

IETF - Internet Engineering Task Force. Formed in 1986 when the Internet was evolving from a Defense Department experiment into an academic network, the IETF is one of two technical working bodies of the Internet Activities Board.

IGMP - Internet Group Management Protocol. A protocol used by IP hosts and gateways to report to report their multicast group memberships. When used in concert with a multicast protocol, the IP based network can support multicasting.

IGP - Interior Gateway Protocol. The protocol used to exchange routing information between collaborating routers in the Internet. RIP, EIGRP, and OSPF are examples IGPs.

Internet2 - High-speed network created by a consortium of U.S. universities called the University Corporation for Advanced Internet Development (UCAID). It transmits high quality audio and video with almost no delay. Internet2 serves as a private Internet for the exclusive use of its member organizations and is separated from the traditional Internet.

IP - Internet Protocol. IP is the most important of the protocols on which the Internet is based. The IP Protocol is a standard describing software that keeps track of the Internet's addresses for different nodes, routes outgoing messages, and recognizes incoming messages. It allows a packet to traverse multiple networks on the way to its final destination. Originally developed by the Department of Defense to support interworking of dissimilar computers across a network.

IPS - Intrusion Prevention System. An IPS integrates with an IDS to automate network responses to many network attacks. An IPS provides two types of prevention: reactive and proactive. Reactive prevention simply acts once an attack has actually been detected. Proactive prevention occurs before any attacks occur. Once a harmful event has been identified systems automatically take action.

IPSec - A collection of IP security measures that comprise an optional tunneling protocol for IP. IPsec supports authentication through an "authentications header" which is used to verify the validity of the originating address in the header of every packet of a packet stream.

ISP - Internet Service Provider. A vendor who provides commodity access for customers (companies) to the Internet and the World Wide Web.

ISR - Cisco's Integrated Service Router series. These routers have built in IPS functions.

IXC - IntereXchange Carrier. Also known as IEC (InterExchange Carrier) and IC. Long-haul long distance carrier.

HSRP - Hot Standby Routing Protocol, a proprietary routing protocol from Cisco for fault-tolerant IP routing. HSRP enables a set of routers to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN.

LAN - Local Area Network. A fancy name for a communications network connecting personal computers, workstations, printers, file servers and other devices inside a campus building.

LATA - Local Access and Transport Area. One of the 196 local geographical areas in the US within which a local telephone company may offer telecommunications services, local or long distance. i.e. InterLATA Services, traffic or facilities that originate in one LATA, crossing over and terminating in another Local Access and Transport Area. This can be either Interstate or Intrastate service, traffic or facilities.

MAN - Metropolitan Area Network. A high-speed intra-city data network that links multiple locations within a campus, city or LATA. Typically extends as far as 50Km.

OC3 - SONET Level with a line rate of 155.52Mbps with a capacity of 28DS1 or 1 DS3.

OC12 - SONET Level with a line rate of 622.08Mbps with a capacity of 336DS1 or 12 DS3.

OC48 - SONET Level with a line rate of 2.488Gbps with a capacity of 1,344DS1 or 48 DS3.

OC192 - SONET Level with a line rate of 9.853Gbps with a capacity of 5,376DS1 or 192 DS3.

OC768 - SONET Level with a line rate of 39.812Gbps with a capacity of 21,504DS1 or 768 DS3.

OTP - One Time Password.

OSI - Open Systems Interconnection. A reference model developed by the ISO (International Organization or Standardization, as translated into English). The OSI reference model is the only internationally accepted framework of standard for communication between different systems made by different vendors. ISO's goal is to create an open systems networking environment where any vendor's computer system, connected to any network and can freely share data with any other computer system on that network or linked network.

PI - Performance Indicator.

PIM - Protocol Independent Multicast. Multicasting is the process of sending one packet to many people without having to duplicate the packet at the source for each recipient. Multicast is often used for multimedia transmissions such as streaming video or sound.

POE - Power Over Ethernet. Standard 802.3af. This IEEE standard is designed to power network devices over Ethernet wiring. This standard defines two types of power sourcing equipment, end-span and mid-span. The major objective of this new standard is to make deploying IP telephones and wireless access points easier and reduce the cost of powering the devices.

POP - Point of Presence. The IXC equivalent of a local phone company's central office. The POP is a long distance carrier's office in your local community.

PPP - Point-to-Point Protocol. PPP is a layer 2, or Data Link Layer (DLL) protocol that allows two peer devices (e.g. two host computers, or a host computer and a bridge or router) to transport packets over a simple link. PPP commonly is used to support TCP/IP traffic between two links.

PSTN - Public Switched Telephone Network. PSTN is the concentration of the world’s public circuit-switched telephone networks, in much the same way that the Internet is the

concentration of the world's public IP-based packet-switched networks. Originally a network of fixed analog telephone systems, the PSTN is now almost entirely digital, and now includes mobile as well as fixed telephones. The PSTN is largely governed by technical standards created by the ITU-T, and uses E.163/E.164 addresses (known more commonly as telephone numbers) for addressing.

QoS - Quality of Service is a measure of the telecommunications - voice, data and/ or video - service quality provided to a subscriber. QoS is easier to define in digital circuits, because you can assign specific error conditions and compare them. QoS is a way to provide better or stable service for select network traffic through bandwidth or latency control.

RFC **-** Request for comment. The development of TCP/IP standards, procedures and specification is done via this mechanism. RFCs are documents that progress through several development stages, under the control of IETF, until they are finalized or discarded.

Route Summarization – Detailed routing information is kept localized, while summary route information is distributed to the rest of the network. For example, not all routers need to know about every route within the network. Some routers such as at a remote office, which have a single connection, only need to know about the route of the next upstream router. A sub-set or route summarization of only those routes needed is distributed to the remote office router, minimizing bandwidth consumption and optimizing router efficiency.

SIP - Session Initiation Protocol. SIP is the emerging standard for setting up telephone calls, multimedia conferencing and other types of real-time communications on the Internet. SIP is touted as much faster, more scalable and easier to implement than H.323. An array of network gear including IP phones, IP PBXs, servers, media gateways and soft switches support SIP. SIP is the Application Layer (Layer 7 of the OSI model) protocol for the establishment, modification and termination of conferencing and telephony sessions over an IP based network(s).

SONET - Synchronous Optical NETwork. A family of fiber optic transmission rates. Created to provide the flexibility needed to transport many digital signals with different capacities, and to provide a design standard for manufacturers. SONET is an optical interface standard that allows interlocking of transmission products from multiple vendors. The levels are described in OC level.

T1 - A digital transmission link with a signaling speed of 1.544 Mbps (1.544,000 bits per second) in both directions (i.e. send and receive). T1 is a standard for digital transmission in North America. The T1 can be divided up into 24 channels of 64K each.

TKIP - Temporal Key Integrity Protocol. A security protocol used in Wi-Fi Protected Access (WPA). TKIP ensures that every packet is sent with its own unique encryption key.

TRUNK - A type of data circuit used in a LAN environment where 802.1Q tagging information is appended allowing multiple VLANs to be sent.

VLAN - Virtual Local Area Network. A VLAN in a switched network is a collection of devices grouped together to form a virtual network within a larger network. VLANs allow an administrator to create networks based on parameters beyond the network address hence the name "virtual".

VoIP - Voice over Internet Protocol. VoIP is the routing of voice conversations over the Internet or through any other IP-based network.

VPN - Virtual Private Network. A private communications network often used within a company, or by several companies or organizations, to communicate confidentially over a public accessible network (i.e. the Internet). VPN is a cost effective and secure way for different corporations to provide user access to the corporate network and for remote networks to communicate with each other across the Internet.

WAN - Wide Area Network. A public voice or data network that extends beyond the metropolitan area. WANs are used to connect local area networks (LANs) together, so that users and computers in one location can communicate with users and computers in another location. The largest and most well known example of a WAN is the Internet.

WINS - Windows Internet Naming Service. WINS is Microsoft's implementation of NetBIOS Name Server (NBNS) on Windows. A name server and service for NetBIOS computer names. Example, it is to NetBIOS names what DNS is to domain names, a central mapping of host names to network addresses.

WLAN - Wireless Local Area Network. A LAN without wires. A WLAN is the linking of two or more computers without using wires.

WPA - Wi-Fi Protected Access (WPA) is an industry standard based on a subset of an early draft of the IEEE 802.11i specification, Robust Security Network for WLANs. WPA has replaced WEP (Wired Equivalent Privacy), which proved too easy to compromise. WPA replaces WEP keying mechanism with the more robust TKIP (Temporal Key Integrity Protocol), adds a strong message integrity check and supports authentication using 802.1X.

6.2 INDEX OF FIGURES